(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年7 月29 日 (29.07.2004)

PCT

(10) 国際公開番号
WO 2004/064317 A1

(51) 国際特許分類[7]: H04L 9/32, G11B 20/10, G06F 12/14

(21) 国際出願番号: PCT/JP2003/016226

(22) 国際出願日: 2003 年12 月18 日 (18.12.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-6915 2003 年1 月15 日 (15.01.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川 6 丁目 7 番 3 5 号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 木谷 聡 (KITANI,Satoshi) [JP/JP]; 〒141-0001 東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 村松 克美 (MURAMATSU,Katsumi) [JP/JP]; 〒141-0001 東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 杉浦 正知, 外(SUGIURA,Masatomo et al.); 〒171-0022 東京都 豊島区 南池袋 2丁目49番 7号 池袋パークビル 7 階 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

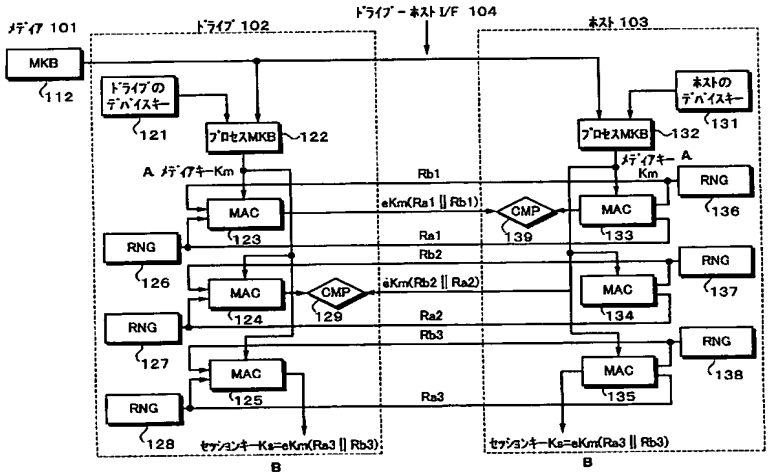
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

[続葉有]

(54) Title: MUTUAL AUTHENTICATION METHOD, PROGRAM, RECORDING MEDIUM, SIGNAL PROCESSING SYSTEM, REPRODUCTION DEVICE, AND INFORMATION PROCESSING DEVICE

(54) 発明の名称: 相互認証方法、再生装置及び情報処理装置



101...MEDIUM
102...DRIVE
103...HOST
104...DRIVE-HOST I/F
121...DRIVE DEVICE KEY
122...PROCESS MKB
A...MEDIUM KEY Km
B...SESSION KEY Ks=eKm(Ra3 || Rb3)
131...HOST DEVICE KEY
132...PROCESS MKB

(57) Abstract: An MKB and a device key (121) of a drive are input to a process MKB. The drive is subjected to revoke processing and a host (103) is revoked by a process MKB (132). MAC values calculated by MAC calculation blocks (123, 133) are compared in the host (103). If the two values are judged to be identical, the authentication of the drive (102) by the host (103) is successful. MAC values calculated

[続葉有]

WO 2004/064317 A1

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

by MAC calculation blocks (134, 124) of the host (103) are compared in the drive (102). If the two values are judged to be identical, authentication of the host (103) by the drive (102) is successful. When the mutual authentication is successful, a common session key is generated by MAC calculation blocks (125, 135).

(57) 要約: プロセスＭＫＢ１２２にＭＫＢとドライブの持つデバイスキー１２１とが入力され、ドライブがリボーク処理され、プロセスＭＫＢ１３２によってホスト１０３がリボーク処理される。ＭＡＣ演算ブロック１２３および１３３が演算したＭＡＣ値がホスト１０３内において比較され、二つの値が同一と判定されると、ホスト１０３によるドライブ１０２の認証が成功したことになる。ホスト１０３のＭＡＣ演算ブロック１３４および１２４が演算したＭＡＣ値がドライブ１０２内において比較され、二つの値が同一と判定されると、ドライブ１０２によるホスト１０３の認証が成功したことになる。相互認証が成功すると、ＭＡＣ演算ブロック１２５および１３５によって、共通のセッションキーが生成される。

相互認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置

技術分野

この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディアに暗号化コンテンツを記録し、また、ディスクメディアから暗号化コンテンツを再生する場合に適用される相互認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置に関する。

背景技術

近年開発されたＤＶＤ(Digital Versatile Disc)等の記録媒体では、１枚の媒体に例えば映画１本分の大量のデータをディジタル情報として記録することが可能である。このように映像情報等をディジタル情報として記録することが可能となってくると不正コピーを防止して著作権の保護を図ることがますます重要となっている。

ＤＶＤ－Video では、コピープロテクション技術としてＣＳＳ(Content Scrambling System) が採用されている。ＣＳＳは、ＤＶＤ－ＲＯＭメディアに対する適用のみが認可されており、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷ、ＤＶＤ＋Ｒ、ＤＶＤ＋ＲＷ等の記録型ＤＶＤでのＣＳＳの利用がＣＳＳ契約によって禁止されている。したがって、ＣＳＳ方式で著作権保護されたＤＶＤ－Video の内容を記録型ＤＶＤへのまるごとコピー（ビットバイビットコピー）することは、ＣＳＳ契約上では、認められた行為ではない。

しかしながら、ＣＳＳの暗号方式が破られる事態が発生した。ＣＳＳの暗号化を解除してＤＶＤ－Video の内容を簡単にハードディスクにコピーすることを可能とする「ＤｅＣＳＳ」と呼ばれるソフトウェアがインターネット上で配布された。「ＤｅＣＳＳ」が出現した背景には、本来耐タンパー化が義務付けられているはずのＣＳＳ復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的にＣＳＳアルゴリズム全体が解読された経緯がある。

ＣＳＳの後に、ＤＶＤ－Audio 等のＤＶＤ－ＲＯＭの著作権保護技術であるＣＰＰＭ(Content Protection for Pre-Recorded Media)、並びに記録型ＤＶＤ、メモリカードに関する著作権保護技術ＣＰＲＭ(Content Protection for Recordable Media) が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、システムを更新でき、データをまるごとコピーしても再生を制限できる特徴を有している。ＤＶＤに関する著作権保護の方法に関しては、下記の非特許文献１に説明され、ＣＰＲＭは、ライセンス管理者である米4C Entity,LLC が配布する下記の資料に説明されている。

山田，「ＤＶＤを起点に著作権保護空間を広げる」，日経エレクトロニクス 2001.8.13,p.143-153

"Content Protection for Recordable Media Specification DVD Book"、インターネット＜ＵＲＬ：http://www.4Centity.com/＞

パーソナルコンピュータ（以下、適宜ＰＣと略す）環境下では、ＰＣとドライブとが標準的インターフェースで接続されるために、標準的インターフェースの部分で秘密保持が必要なデータが知られたり、データが改ざんされるおそれがある。アプリケーションソフトウェア

がリバースエンジニアリングされ、秘密情報が盗まれたり、改ざんされる危険がある。このような危険性は、記録再生装置が一体に構成された電子機器の場合では、生じることが少ない。

著作権保護技術をＰＣ上で実行されるアプリケーションプログラムへ実装する際には、その著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的である。しかしながら、耐タンパー性の強度を示す指標がない。その結果、どの程度のリバースエンジニアリングへの対応を行うかは、インプレメンターの個々の判断や能力に委ねられているのが現状である。ＣＳＳの場合は、結果としてその著作権保護技術が破られてしまった。ＣＳＳの後に提案されたＣＰＰＭおよび記録型ＤＶＤに関する著作権保護技術ＣＰＲＭにおいても、既に破られているＣＳＳに新たな機能を加えたものであり、また、著作権保護技術に関わるアルゴリズムは、大部分がＰＣでの実装に依存するものであり、コンテンツプロテクションの機能が充分に強いものと言えない問題があった。すなわち、アプリケーションソフトウェアなどのリバースエンジニアリングによって、著作権保護技術に関わる秘密情報の解析により暗号方式が破られ、ディスクからのデータとしてＰＣがそのまま読み出した暗号化コンテンツが「ＤｅＣＳＳ」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を招くことで、著作権保護が機能しなくなるという危険性があった。

この発明の目的は、ＰＣ環境下でも著作権保護技術の安全性を確保することができる相互認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置を提供することにある。

発明の開示

上述した課題を解決するために、この発明の第１の態様は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法において、

再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第１の判定ステップを有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定ステップを有し、

第１の判定ステップによって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、第２の判定ステップによって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法である。

この発明の第２の態様は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムであって、

再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第１の判定ステップを有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情

報を用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定ステップを有し、

第１の判定ステップによって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、第２の判定ステップによって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプログラムである。

この発明の第３の態様は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムを格納した記録媒体であって、

再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第１の判定ステップを有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定ステップを有し、

第１の判定ステップによって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、第２の判定ステップによって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプログラムを格納した記録媒体である。

この発明の第４の態様は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置とを備える信号処理システムであって、

再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第１の判定手段を有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定手段を有し、

第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証手段と、

相互認証手段による相互認証後に、再生装置および情報処理装置に共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする信号処理システムである。

この発明の第５の態様は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有し、コンテンツ情報が伝達手段を介して情報処理装置に送信され、処理される信号処理システムにおける再生装置であって、

当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第１の判定手段を有し、

第１の判定手段によって無効化すべきという判定をされなかった場

合に生成される第１の鍵情報と、

情報処理装置に設けられている当該情報処理装置を表す情報とリボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、情報処理装置と相互に認証する相互認証手段と、

相互認証手段による相互認証後に、情報処理装置と共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする再生装置である。

この発明の第６の態様は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、再生装置がコンテンツ情報を読み出し、コンテンツ情報が伝達手段を介して受信され、処理される情報処理装置であって、

再生装置に設けられている第１の判定手段によって、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定し、第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、

当該情報処理装置を表す情報とリボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定手段を有し、

第１の鍵情報と、第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、再生装置と相互に認証する相互認証手段と、

相互認証手段による相互認証後に、再生装置と共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする情報処理装置である。

この発明では、メディア上に記録された鍵情報（ＭＫＢ）と各デバイスまたは各アプリケーションに記憶されている鍵情報（デバイスキー）から同一の値として導かれる鍵情報（メディアキー）を利用して相互認証がなされる。したがって、この発明においては、認証のためだけに用意される特定の認証鍵を必要とせず、秘密情報を少なくでき、また、デバイスまたはアプリケーションによってデバイスキーを異ならせることが可能であるので、秘密情報が不正に読み取られる危険性を少なくできる。

この発明では、著作権保護技術に関する秘密情報である電子機器またはアプリケーションソフトウェア固有の情報例えばデバイスキーがドライブ内に実装されているので、情報処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばＬＳＩによって生成できるので、ＰＣ内でソフトウェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少なくできる。

図面の簡単な説明

第１図は、先に提案されているレコーダ、プレーヤおよびＤＶＤメ

ディアからなるシステムを説明するためのブロック図である。

第2図は、ＰＣベースのＤＶＤメディア記録再生システムを説明するためのブロック図である。

第3図は、第2図のシステムにおけるＤＶＤドライブ4およびホスト5の処理の手順を説明するための略線図である。

第4図は、第2図のシステムにおける認証動作を説明するためのフローチャートである。

第5図は、この発明の一実施形態による相互認証のための構成を示すブロック図である。

第6図は、この発明の一実施形態におけるドライブの認証動作の処理の手順を説明するためのフローチャートである。

第7図は、この発明の一実施形態におけるホストの認証動作の処理の手順を説明するためのフローチャートである。

第8図は、この発明の一実施形態によるドライブとホストを組み合わせたレコーダの構成の一例をブロック図である。

第9図は、レコーダの一例の通信の手順を説明するための略線図である。

第１０図は、この発明の一実施形態によるドライブとホストを組み合わせたプレーヤの構成の一例をブロック図である。

第１１図は、プレーヤの一例の通信の手順を説明するための略線図である。

第１２図は、この発明の一実施形態によるドライブとホストを組み合わせたレコーダの構成の他の例をブロック図である。

第１３図は、レコーダの他の例の通信の手順を説明するための略線図である。

発明を実施するための最良の形態

この発明の一実施形態の説明に先立って、本明細書の特許請求の範囲において使用される用語と実施の形態中で使用される用語との対応関係について以下に説明する。

記録媒体：メディア例えばディスク、再生装置：ドライブ、情報処理装置：ホスト、伝達手段：ドライブーホストインターフェース、信号処理システム：メディアを再生するドライブとホストとがドライブーホストインターフェースを介して接続されるシステムである。第1の送信手段：ドライブ側からセッションキーを共通鍵とした共通鍵暗号方式で情報をホスト側に送る手段、第2の送信手段：逆にホスト側からセッションキーを共通鍵として情報をドライブ側に送る手段のことである。

コンテンツ情報：メディアに記録されている情報または記録すべき情報をコンテンツ情報としている。リボケーション情報：メディアに予め記録されているメディアキーブロックＭＫＢ(Media Key Blocks)、記録媒体固有の情報：メディアＩＤ、デバイスキー：再生装置または情報処理装置を表す情報、装置を無効化すべきか否かを判定する判定手段：プロセスＭＫＢである。プロセスＭＫＢでは、ドライブ側の第1の判定手段によりドライブが無効化されなければ、ドライブ側のメディアキーとして第1の鍵情報が生成され、ホスト側の第2の判定手段によりホストが無効化されなければ、ホスト側のメディアキーとして第2の鍵情報が生成される。ドライブとホストは、独立して無効化が可能であり、無効化された場合は、期待されるメディアキーを得ることができないので「第1の」、「第2の」と分けている。

相互認証手段：ＡＫＥ(Authentication and Key Exchange)（プロセスＭＫＢ以降の乱数交換、ＭＡＣ計算、比較からなるドライブ側の

第１の確認手段とホスト側の第２の確認手段により相互に相手の動作を確認することである。ドライブ側とホスト側の何れが先に確認するかの順番は、任意であるので、用語の統一を図るために、ドライブ側の確認手段を「第１の」としている。）

共通鍵：セッションキー（確実に暗号化・復号に使われるセッションキーとコンテンツキーとは、「鍵」でそれ以外は「鍵情報」としている。認証完了後なので共通鍵として同じ暗号化鍵が生成されるが、生成している装置と、基にしている鍵情報の呼び方を変えていることから、ドライブ側の生成手段を第１の共通鍵生成手段、ホスト側の生成手段を第２の共通鍵生成手段としている。）

乱数を生成する乱数生成手段：乱数発生器（ＲＮＧ：Random Number Generator）（ドライブ側の乱数生成手段を第１の乱数生成手段、ホスト側の乱数生成手段を第２の乱数生成手段とし、特許請求の範囲においては、生成される乱数に対して請求の範囲に出てくる順番で番号をつけている。）

所定の計算を行う計算手段：ＭＡＣ(Message Authentication Code）演算ブロック（乱数交換手段により交換された乱数を用いて、ドライブ側で計算する手段を第１の計算手段、ホスト側の計算手段を第２の計算手段としている。）

比較手段：比較（ドライブ側の比較を第１の比較手段、ホスト側の比較を第２の比較手段としている。）

記録媒体固有の鍵情報：メディアユニークキー（本実施形態においては、メディアユニークキーの生成は耐タンパー性を持たせるために全てドライブ側で行われているので、記録媒体固有の鍵情報（メディアユニークキー）を生成する中間鍵生成手段は、ドライブ側のみとしている。）

コンテンツ情報暗号化鍵またはコンテンツ情報復号鍵の基になる鍵情報：（記録時に使われるタイトルキーを第３の鍵情報、再生時に使われるタイトルキーを第４の鍵情報としている。メディアユニークキーによってタイトルキーを暗号化する手段を鍵情報暗号化手段、復号する手段を鍵情報復号手段としている。メディアユニークキーによって暗号化されたタイトルキーを記録媒体に記録する手段を暗号化鍵情報記録手段としている。）

コンテンツ情報を暗号化または復号するための鍵：コンテンツキー（記録時に使われるコンテンツキーをコンテンツ情報暗号化鍵とし、再生時に使われるコンテンツキーをコンテンツ情報復号鍵としている。コンテンツ情報暗号化鍵を生成する手段を最終暗号化鍵生成手段、コンテンツ情報復号鍵を生成する手段を最終復号鍵生成手段としている。暗号化されたコンテンツ情報を記録媒体に記録する手段をコンテンツ情報記録手段とし、暗号化されたコンテンツ情報を復号する手段をコンテンツ情報復号手段としている。）

次に、この発明の理解の容易のために、最初に第1 図を参照して著作権保護技術例えばＤＶＤ用ＣＰＲＭのアーキテクチャについて説明する。第１図において、参照符号１が例えばＣＰＲＭ規格に準拠したＤＶＤ－Ｒ／ＲＷ、ＤＶＤ－ＲＡＭ等の記録型ＤＶＤメディアを示す。参照符号２が例えばＣＰＲＭ規格に準拠したレコーダを示す。参照符号３が例えばＣＰＲＭ規格に準拠したプレーヤを示す。レコーダ２およびプレーヤ３は、機器またはアプリケーションソフトウェアである。

未記録ディスクの状態において、ＤＶＤメディア１の最内周側のリードインエリアのＢＣＡ(Burst Cutting Area)またはＮＢＣＡ(Narrow Burst Cutting Area) と称されるエリアには、メディアＩＤ１１が

記録されている。リードインエリアのエンボスまたはプリ記録データゾーンには、メディアキーブロック（以下、ＭＫＢと適宜略す）１２が予め記録されている。メディアＩＤ１１は、個々のメディア単位例えばディスク１枚毎に異なる番号であり、メディアの製造者コードとシリアル番号から構成される。メディアＩＤ１１は、メディアキーを個々のメディアで異なるメディアユニークキーへ変換する際に必要となる。メディアキーブロックＭＫＢは、メディアキーの導出、並びに機器のリボケーション（無効化）を実現するための鍵束である。これらのメディアＩＤおよびメディアキーブロックは、記録媒体固有の第１の情報である。

ディスク１の書き換えまたは追記可能なデータ領域には、コンテンツキーで暗号化された暗号化コンテンツ１３が記録される。暗号化方式としては、Ｃ２(Cryptomeria Ciphering) が使用される。

ＤＶＤメディア１には、暗号化タイトルキー１４およびＣＣＩ(Copy Control Information)１５が記録される。暗号化タイトルキー１４は、暗号化されたタイトルキー情報であり、タイトルキー情報は、タイトル毎に付加される鍵情報である。ＣＣＩは、コピーノーモア、コピーワンス、コピーフリー等のコピー制御情報である。

レコーダ２は、デバイスキー２１、プロセスＭＫＢ２２、Ｃ２＿Ｇ２３、乱数発生器２４、Ｃ２＿Ｅ２５、Ｃ２＿Ｇ２６およびＣ２＿ＥＣＢＣ２７の構成要素を有する。プレーヤ３は、デバイスキー３１、プロセスＭＫＢ３２、Ｃ２＿Ｇ３３、Ｃ２＿Ｄ３５、Ｃ２＿Ｇ３６およびＣ２＿ＤＣＢＣ３７の構成要素を有する。

デバイスキー２１、３１は、個々の装置メーカ、またはアプリケーションソフトウェアベンダー毎に発行された識別番号である。デバイスキーは、ライセンス管理者によって正当な電子機器またはアプリケ

ーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報である。ＤＶＤメディア１から再生されたＭＫＢ１２とデバイスキー２１とがプロセスＭＫＢ２２において演算されることによって、リボケーションされたかどうかの判別ができる。レコーダ２におけるのと同様に、プレーヤ３においても、ＭＫＢ１２とデバイスキー３１とがプロセスＭＫＢ３２において演算され、リボケーションされたかどうかの判別がなされる。

さらに、プロセスＭＫＢ２２、３２のそれぞれにおいて、ＭＫＢ１２とデバイスキー２１、３１からメディアキーが算出される。ＭＫＢ１２の中にレコーダ２またはプレーヤ３のデバイスキーが入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキーを持つレコーダ２またはプレーヤ３が正当なものでないと判断される。すなわち、そのようなレコーダ２またはプレーヤ３がリボケーションされる。

Ｃ２＿Ｇ２３、３３は、それぞれ、メディアキーとメディアＩＤとを演算し、メディアユニークキーを導出する処理である。

乱数発生器（ＲＮＧ：Random Number Generator）２４は、タイトルキーの生成に利用される。乱数発生器２４からのタイトルキーがＣ２＿Ｅ２５に入力され、タイトルキーがメディアユニークキーで暗号化される。暗号化タイトルキー１４がＤＶＤメディア１に記録される。

プレーヤ３では、ＤＶＤメディア１から再生された暗号化タイトルキー１４とメディアユニークキーとがＣ２＿Ｄ３５に供給され、暗号化タイトルキーがメディアユニークキーで復号され、タイトルキーが得られる。

レコーダ２においては、ＣＣＩとタイトルキーとがＣ２＿Ｇ２６に

供給され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＥＣＢＣ２７に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ１３がＤＶＤメディア１に記録される。

プレーヤ３においては、ＣＣＩとタイトルキーとがＣ２＿Ｇ３６に供給され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＥＣＢＣ３７に供給され、ＤＶＤメディア１から再生された暗号化コンテンツ１３がコンテンツキーを鍵として復号される。

第１図の構成において、レコーダ２による記録の手順について説明する。レコーダ２は、ＤＶＤメディア１からＭＫＢ１２を読み出し、プロセスＭＫＢ２２によってデバイスキー２１とＭＫＢ１２とを演算し、メディアキーを計算する。演算結果が予め定められた値を示すならば、デバイスキー２１（レコーダ２の機器またはアプリケーション）がＭＫＢによってリボークされたと判定される。レコーダ２は、以後の処理を中断し、ＤＶＤメディア１への記録を禁止する。若し、メディアキーの値が予め定められた値以外であれば、処理を継続する。

レコーダ２は、ＤＶＤメディア１からメディアＩＤ１１を読み、メディアキーと共にメディアＩＤをＣ２＿Ｇ２３に入力しメディア毎に異なるメディアユニークキーが演算される。乱数発生器２４で発生させたタイトルキーがＣ２＿Ｅ２５で暗号化され、暗号化タイトルキー１４としてＤＶＤメディア１に記録される。タイトルキーとコンテンツのＣＣＩ情報がＣ２＿Ｇ２６で演算され、コンテンツキーが導出される。コンテンツキーでコンテンツをＣ２＿ＥＣＢＣ２７で暗号化し、ＤＶＤメディア１上に暗号化コンテンツ１３としてＣＣＩ１５と共に記録する。

プレーヤ３による再生の手順について説明する。最初にＭＫＢ１２をＤＶＤメディア１から読み出す。デバイスキー３１とＭＫＢ１２を演算し、リボケーションの確認がなされる。デバイスキー３１、すなわち、プレーヤ３の機器またはアプリケーションがリボークされない場合には、メディアＩＤを使用してメディアユニークキーが演算され、読み出された暗号化タイトルキー１４とメディアユニークキーからタイトルキーが演算される。タイトルキーとＣＣＩ１５とがＣ２＿Ｇ３６に入力され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＤＣＢＣ３７に入力され、コンテンツキーを鍵として、ＤＶＤメディア１から再生された暗号化コンテンツ１３に対してＣ２＿ＤＣＢＣ３７の演算が施される。その結果、暗号化コンテンツ１３が復号される。

このように、コンテンツの復号に必要なコンテンツキーを得るためには、ＤＶＤメディアの１枚毎に異なるメディアＩＤが必要となるので、たとえメディア上の暗号化コンテンツが忠実に他のメディアにコピーされても、他のメディアのメディアＩＤがオリジナルのメディアＩＤと異なるために、コピーされたコンテンツを復号することができず、コンテンツの著作権を保護することができる。

上述した第１図の構成は、記録再生機器として構成されたものである。この発明は、ＤＶＤメディア１に対するコンテンツ保護処理をＰＣ環境下で扱う場合に適用される。第２図を参照して現行の方式によるＰＣとドライブの役割分担を示す。第２図において、参照符号４が上述したＣＰＲＭ規格に準拠したＤＶＤメディア１を記録および再生する記録再生装置としてのＤＶＤドライブを示す。

参照符号５がデータ処理装置としてのホスト例えばＰＣを示す。ホスト５は、ＤＶＤメディア１に記録可能で、ＤＶＤメディア１から再

生可能なコンテンツを扱うことができ、且つＤＶＤドライブ４と接続されてデータ交換が可能な装置またはアプリケーションソフトウェアである。例えばＰＣに対してアプリケーションソフトウェアがインストールされることによってホスト５が構成される。

ＤＶＤドライブ４とホスト５との間がインターフェース４ａで接続されている。インターフェース４ａは、ＡＴＡＰＩ(AT Attachment with Packet Interface)，ＳＣＳＩ(Small Computer System Interface)，ＵＳＢ(Universal Serial Bus)，ＩＥＥＥ(Institute of Electrical and Electronics Engineers) １３９４等である。

ＤＶＤメディア１には、メディアＩＤ１１、メディアキーブロック１２およびＡＣＣ(Authentication Control Code) が予め記録されている。ＡＣＣは、ＤＶＤドライブ４とホスト５との間の認証がＤＶＤメディア１によって異なるようにするために予めＤＶＤメディア１に記録されたデータである。

ＤＶＤドライブ４は、ＡＣＣ１６をＤＶＤメディア１から読み出す。ＤＶＤメディア１から読み出されたＡＣＣ１６がＤＶＤドライブ４のＡＫＥ(Authentication and Key Exchange) ４１に入力されると共に、ホスト５へ転送される。ホスト５は、受け取ったＡＣＣをＡＫＥ５１に入力する。ＡＫＥ４１および５１は、乱数データを交換し、この交換した乱数とＡＣＣの値とから認証動作の度に異なる値となる共通のセッションキー（バスキーと称する）を生成する。

バスキーがＭＡＣ(Message Authentication Code) 演算ブロック４２および５２にそれぞれ供給される。ＭＡＣ演算ブロック４２および５２は、ＡＫＥ４１および５１でそれぞれ得られたバスキーをパラメータとして、メディアＩＤおよびメディアキーブロック１２のＭＡＣを計算するプロセスである。ＭＫＢとメディアＩＤの完全性(integri

ty）をホスト５が確認するために利用される。

ＭＡＣ４２および５２によってそれぞれ計算されたＭＡＣがホスト５の比較５３において比較され、両者の値が一致するかどうかが判定される。これらのＭＡＣの値が一致すれば、ＭＫＢとメディアＩＤの完全性が確認されたことになる。比較出力でスイッチＳＷ１が制御される。

スイッチＳＷ１は、ＤＶＤドライブ４のＤＶＤメディア１の記録または再生経路と、ホスト５の暗号化／（または）復号モジュール５４との間の信号路をＯＮ／ＯＦＦするものとして示されている。スイッチＳＷ１は、信号路のＯＮ／ＯＦＦを行うものとして示されているが、より実際には、ＯＮの場合にホスト５の処理が継続し、ＯＦＦの場合にホスト５の処理が停止することを表している。暗号化／復号モジュール５４は、メディアユニークキーと暗号化タイトルキーとＣＣＩとからコンテンツキーを算出し、コンテンツキーを鍵としてコンテンツを暗号化コンテンツ１３へ暗号化し、またはコンテンツキーを鍵として暗号化コンテンツ１３を復号する演算ブロックである。

メディアユニークキー演算ブロック５５は、ＭＫＢ１２とメディアＩＤとデバイスキー５６とからメディアユニークキーを演算する演算ブロックである。第１図に示すレコーダまたはプレーヤと同様に、デバイスキーとＭＫＢ１２とからメディアキーが演算される。メディアキーとメディアＩＤ１１とからメディアユニークキーが演算される。メディアキーが所定の値となった場合には、その電子機器またはアプリケーションソフトウェアが正当なものではないと判断され、リボークされる。したがって、メディアユニークキー演算ブロック５５は、リボケーションを行うリボーク処理部としての機能も有する。

記録時に、比較５３によって完全性が確認された場合には、スイッ

チＳＷ１がＯＮされる。号化／復号モジュール５４からスイッチＳＷ１を通じてドライブ４に対して、暗号化コンテンツ１３、暗号化タイトルキー１４およびＣＣＩ１５が供給され、ＤＶＤメディア１に対してそれぞれ記録される。再生時に、比較５３によって完全性が確認された場合には、スイッチＳＷ１がＯＮされる。ＤＶＤメディア１からそれぞれ再生された暗号化コンテンツ１３、暗号化タイトルキー１４およびＣＣＩ１５がスイッチＳＷ１を通じてホスト５の暗号化／復号モジュール５４に対して供給され、暗号化コンテンツが復号される。

第３図は、第２図に示す現行のＰＣ環境下のＤＶＤメディアを利用するシステムにおいて、ＤＶＤメディア１と、ＤＶＤドライブ４と、ホスト５との間の信号の授受の手順を示す。ホスト５がＤＶＤドライブ４に対してコマンドを送り、ＤＶＤドライブ４がコマンドに応答した動作を行う。

ホスト５からの要求に応じてＤＶＤメディア１上のＡＣＣがシークされ、読み出される（ステップＳ１）。次のステップＳ２において、読み出されたＡＣＣがＡＫＥ４１に入力されると共に、ホスト５へ転送され、ホスト５では、受け取ったＡＣＣがＡＫＥ５１へ入力される。ＡＫＥ４１および５１は、乱数データを交換し、この交換した乱数とＡＣＣ１６の値から認証動作の度に異なる値となるセッションキーとしてのバスキーを生成し、バスキーをＤＶＤドライブ４とホスト５が共有する。相互認証が成立しなかった場合では、処理が中断する。

認証動作は、電源のＯＮ後のディスク検出時並びにディスクの交換時には、必ず行われる。記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うよう

にしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

認証が成功すると、ステップＳ３において、ホスト５がＤＶＤドライブ４に対して、ＤＶＤメディア１からのＭＫＢ（メディアキーブロック）パック＃０の読み出しを要求する。ＭＫＢは、パック０～パック１５の１６セクタが１２回繰り返してリードインエリアに記録されている。パック単位で、エラー訂正符号化がなされている。

ＤＶＤドライブ４がステップＳ４においてＭＫＢのパック＃０を読みに行き、ステップＳ５において、パック＃０が読み出される。ＤＶＤドライブ４は、モディフアイドＭＫＢをホスト５へ戻す（ステップＳ６）。ＭＫＢを読み出す際に、バスキーをパラメータとしてＭＡＣ値を計算し、ＭＫＢに対してＭＡＣ値を付加してホスト５へデータを転送する。パック＃０以外の残りのＭＫＢパックの要求と、ＤＶＤドライブ４の読み出し動作と、モディフアイドＭＫＢパックの転送動作とがＭＫＢのパックがなくなるまで、例えばパック＃１５が読み出され、ホスト５へ転送されるまで、ステップＳ７およびＳ８によって繰り返しなされる。

ホスト５がＤＶＤドライブ４に対してメディアＩＤを要求する。ＤＶＤドライブ４がＤＶＤメディア１に記録されているメディアＩＤを読みに行き、ステップＳ１１において、メディアＩＤが読み出される。ＤＶＤドライブ４は、メディアＩＤを読み出す際に、バスキーをパラメータとしてそのＭＡＣ値を計算する。ＤＶＤドライブ４はステップＳ１２において、読み出されたメディアＩＤに対してＭＡＣ値ｍ１を付加してホスト５へデータを転送する。

ホスト５では、ＤＶＤドライブ４から受け取ったＭＫＢ１２およびメディアＩＤ１１からバスキーをパラメータとして再度ＭＡＣ値を計

算し、計算したＭＡＣ値とＤＶＤドライブ４から受け取ったＭＡＣ値とを比較５３で比較する。両者が一致したならば、正しいＭＫＢおよびメディアＩＤを受け取ったと判定して、スイッチＳＷ１をＯＮに設定して処理を先に進める。逆に両者が一致しなかったならば、ＭＫＢおよびメディアＩＤが改ざんされたものと判定して、スイッチＳＷ１をＯＦＦに設定して処理を中断する。

ステップＳ１３において、ホスト５がＤＶＤドライブ４に対して暗号化コンテンツを要求し、ステップＳ１４において、ＤＶＤドライブ４が暗号化コンテンツを読み出し、ステップＳ１３において、読み出した暗号化コンテンツがホスト５に転送される。ホスト５のメディアユニークキー演算ブロック５５では、デバイスキー５６とＭＫＢ１２とメディアＩＤ１１とによってメディアユニークキーが計算される。メディアユニークキーが暗号化／復号モジュール５４に供給され、暗号化タイトルキー１４、ＣＣＩ１５からコンテンツキーが求められる。コンテンツキーを鍵としてＤＶＤメディア１から読み出された暗号化コンテンツが復号される。ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

第４図のフローチャートにおいて、ステップＳＴ１は、ＭＡＣ演算ブロック４２でバスキーをパラメータとして求められたＭＡＣ計算値と、ＭＡＣ演算ブロック５３でバスキーをパラメータとして求められたＭＡＣ計算値とを比較するステップである。両者が一致すれば、スイッチＳＷ１がステップＳＴ２においてＯＮとされる。両者が一致しない場合では、スイッチＳＷ１がステップＳＴ３においてＯＦＦとされ、処理が停止する。

上述したＣＰＲＭでは、ＤＶＤ－Video の著作権保護技術であるＣＳＳと同じバスキー生成方法を採用している。ＣＳＳ認証方式の内容

は、本来秘密であるべき情報であるが、既に解析され一般ユーザーが入手可能なＣＳＳライセンス管理団体であるDVD-CCA の許諾を得ていないフリーソフトウェアによって動作させることが可能となっている。コンテンツプロテクション処理は、ホスト側でなされる、すなわち、リボケーション判定、メディアキー取得、メディアユニークキー導出、タイトルキー生成・導出からコンテンツキー導出およびコンテンツ暗号化・復号の全てがホスト側の処理であることから、著作権保護技術としての信頼性が低下している。

以下に述べるこの発明は、かかる問題点を解決するものである。一実施形態では、ＰＣ環境下でのコンテンツプロテクション処理におけるＰＣとドライブの役割分担におけるリボケーション動作とメディアキー導出に関わる情報（ここでは、デバイスキー）をドライブ内部に持ち、ＰＣとの相互認証を経てセッションキーを導出するものである。

第５図は、一実施形態における相互認証の構成を示すブロック図であり、第６図は、ドライブ側の処理の流れを示すフローチャートであり、第７図は、ホスト側の処理の流れを示すフローチャートである。以下の説明において、参照符号１０１がメディア例えば光ディスクを示し、参照符号１０２がメディアのドライブを示し、参照符号１０３がドライブ１０２とドライブーホストインターフェース１０４を介して接続されたホストを示す。メディア１０１は、上述したＤＶＤメディアと同様の情報が予め記録されているものである。メディア１０１は、記録可能なものに限らず、読み出し専用のものでも良い。ホスト１０３がドライブ１０２に対して所定のコマンドを送り、その動作を制御する。使用するコマンドは、上述した非特許文献２に記載されているコマンド並びにコマンドを拡張したもの、および、メディア１０

１からコンテンツをセクタ・データとして読み出すためのＲＥＡＤコマンド、メディア１０１へコンテンツをセクタ・データとして書き込むためのＷＲＩＴＥコマンドである。

ドライブ１０２は、ドライブのデバイスキー１２１を有し、ホスト１０３がホストのデバイスキー１３１を有している。デバイスキー１２１は、多くの場合にＬＳＩ(Large Scale Integrated Circuit ：大規模集積回路）内部に配置され、外部から読み出すことができないようセキュアに記憶される。デバイスキー１３１は、ソフトウェアプログラム内にセキュアに記憶される場合と、ハードウェアとしてセキュアに記憶される場合とがある。ドライブ１０２がメディア１０１を扱う正当なドライブとなるためには、一実施形態のように、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成を防止できる効果がある。

第５図に示すように、ドライブ１０２には、ＭＫＢとデバイスキー１２１とが入力され、ドライブのデバイスキーがリボケーションされたかどうかを判定するプロセスＭＫＢ１２２が備えられている。ホスト１０３にも同様に、プロセスＭＫＢ１３２が備えられている。リボケーションされない場合に、プロセスＭＫＢ１２２および１３２からそれぞれメディアキーＫｍが出力される。リボーク判定処理がなされ、メディアキーＫｍが得られてから認証処理がなされる。

参照符号１２３、１２４および１２５は、メディアキーＫｍをパラメータとしてＭＡＣ値を計算するＭＡＣ演算ブロックをそれぞれ示す。また、参照符号１２６、１２７および１２８は、乱数発生器（ＲＮＧ：Random Number Generator ）をそれぞれ示す。乱数発生器１２６が乱数Ｒa1を生成し、乱数発生器１２７が乱数Ｒa2を生成し、乱数発

生器１２８が乱数Ra3を生成する。乱数発生器１２６、１２７、１２８は、例えばＬＳＩの構成の乱数発生器であり、ソフトウェアにより乱数を発生する方法と比較してより真正乱数に近い乱数を発生することができる。乱数発生器を共通のハードウェアとしても良いが、乱数Ra1、Ra2、Ra3は、互いに独立したものである。

ホスト１０３に、メディアキーKmをパラメータとしてＭＡＣ値を計算するＭＡＣ演算ブロック１３３、１３４および１３５と、乱数発生器１３６、１３７および１３８が備えられている。乱数発生器１３６が乱数Rb1を生成し、乱数発生器１３７が乱数Rb2を生成し、乱数発生器１３８が乱数Rb3を生成する。乱数発生器１３６、１３７、１３８は、通常はソフトウェアによって乱数を発生するものであるが、ハードウェアによる乱数が利用できる場合にはこれを用いても良い。

ドライブ１０２において生成された乱数とホスト１０３において生成された乱数とが交換される。すなわち、乱数Ra1および乱数Rb1がＭＡＣ演算ブロック１２３および１３３に入力され、乱数Ra2および乱数Rb2がＭＡＣ演算ブロック１２４および１３４に入力され、乱数Ra3および乱数Rb3がＭＡＣ演算ブロック１２５および１３５に入力される。

ドライブ１０２のＭＡＣ演算ブロック１２３が演算したＭＡＣ値と、ホスト１０３のＭＡＣ演算ブロック１３３が演算したＭＡＣ値とがホスト１０３内の比較１３９において比較され、二つの値が同一か否かが判定される。ここでのＭＡＣ値は、eKm(Ra1‖Rb1)と表記される。ｅＫｍ（）は、メディアキーKmを鍵として括弧内のデータを暗号化することを表している。Ra1‖Rb1の記号は、左側に乱数Ra1を配し、右側に乱数Rb1を配するように、二つの乱数を結合することを表

している。比較の結果、二つの値が同一と判定されると、ホスト１０３によるドライブ１０２の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

ホスト１０３のＭＡＣ演算ブロック１３４が演算したＭＡＣ値と、ドライブ１０２のＭＡＣ演算ブロック１２４が演算したＭＡＣ値とがドライブ１０２内の比較１２９において比較され、二つの値が同一か否かが判定される。ここでのＭＡＣ値は、eKm(Rb2‖Ra2)と表記される。比較の結果、二つの値が同一と判定されると、ドライブ１０２によるホスト１０３の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

かかる相互認証において、比較１３９および１２９の両者において、ＭＡＣ値が同一と判定され、ドライブ１０２およびホスト１０３の両者の正当性が確認されると、すなわち、相互認証が成功すると、ＭＡＣ演算ブロック１２５および１３５によって、共通のセッションキーeKm(Ra3‖Rb3)がそれぞれ生成される。

さらに、上述した相互認証の処理の流れを第６図および第７図のフローチャートを参照して説明する。最初に、第７図のステップＳＴ２０において、ホスト１０３がドライブ１０２に対して、コマンドREPORT KEYを発行し、ＭＫＢの転送を要求する。第６図のステップＳＴ１０において、ドライブ１０２がメディア１０１からＭＫＢ１１２を読み出して、ホスト１０３へ転送する。

次に、ドライブ１０２がステップＳＴ１１において、プロセスＭＫＢ１２２によってメディアキーＫｍを計算し、ホスト１０３がステップＳＴ２１において、プロセスＭＫＢ１３２によってメディアキーＫｍを計算する。この計算の過程でそれぞれが内蔵するデバイスキー１２１および１３１がリボケーションの対象とされているか否かが自分

自身によって確認される（第６図中のステップＳＴ１２、第７図中のステップＳＴ２２）。

ドライブ１０２およびホスト１０３のそれぞれは、リボケーションの対象とされている場合にはリボークされ、処理が終了する。若し、ホスト１０３がリボケーションの対象とされていなければ、ステップＳＴ２３において、コマンドSEND KEYにより、ドライブ１０２に対して乱数発生器１３６および１３７でそれぞれ生成された乱数Rb1と乱数Rb2を転送する。若し、ドライブ１０２がリボケーションの対象とされていなければ、ステップＳＴ１３において、ドライブ１０２がホスト１０３から転送されたこれらの乱数を受け取る。

その後、ホスト１０３は、コマンドREPORT KEYによりドライブ１０２に対してドライブ１０２が持つメディアキーＫｍを鍵としたＭＡＣによるレスポンス値と乱数生成器１２６が発生した乱数Ra1 とをホスト１０３へ転送することを要求する（ステップＳＴ２４）。このレスポンス値は、eKm(Ra1 ‖ Rb1)と表記される。ｅＫｍ（）は、メディアキーＫｍを暗号鍵として括弧内のデータを暗号化することを表している。Ra1 ‖ Rb1の記号は、左側に乱数Ra1を配し、右側に乱数Rb1を配するように、二つの乱数を結合することを表している。

ホスト１０３からコマンドREPORT KEYを受け取ったドライブ１０２は、ステップＳＴ１４において、ＭＡＣ演算ブロック１２３が生成したＭＡＣ値eKm(Ra1 ‖ Rb1)と乱数Ra1をホスト１０３へ転送する。ステップＳＴ２５において、ホスト１０３は、自身のＭＡＣ演算ブロック１３３でＭＡＣ値を計算し、比較１３９においてドライブ１０２から受け取った値と一致するかの確認を行う。若し、受け取ったＭＡＣ値と計算されたＭＡＣ値とが一致したのなら、ホスト１０３によるドライブ１０２の認証が成功したことになる。ステップＳＴ２５におけ

る比較の結果が同一でない場合には、ホスト１０３によるドライブ１０２の認証が失敗したことになり、リジェクト処理がなされる。

ホスト１０３によるドライブ１０２の認証が成功した場合には、ステップＳＴ２６において、ホスト１０３がドライブ１０２へコマンドREPORT KEYを送付し、ドライブ１０２の乱数生成器１２４および１２５がそれぞれ生成する乱数Ｒa2と乱数Ｒa3の転送を要求する。このコマンドに応答して、ステップＳＴ１５において、ドライブ１０２は、これらの乱数をホスト１０３へ転送する。

ステップＳＴ２７において、ホスト１０３のＭＡＣ演算ブロック１３４は、ドライブ１０２から受け取った乱数からホスト１０３が持つメディアキーＫｍを鍵としたＭＡＣによるレスポンス値eKm(Rb2‖Ra2)を計算し、乱数Ｒb3とともに、コマンドSEND KEYを用いてドライブ１０２へ転送する。

ステップＳＴ１６において、ドライブ１０２は、ホスト１０３からレスポンス値eKm(Rb2‖Ra2)および乱数Rb3を受け取ると、自身でＭＡＣ値を計算し、ステップＳＴ１７において、比較１２９によってホスト１０３から受け取ったＭＡＣ値と一致するかの確認を行う。若し、受け取ったＭＡＣ値と計算されたＭＡＣ値とが一致したのなら、ドライブ１０２によるホスト１０３の認証が成功したことになる。この場合には、ステップＳＴ１８において、ＭＡＣ演算ブロック１２５がセッションキーeKm(Ra3‖Rb3)を生成し、また、ホスト１０３に対して認証が成功したことを示す情報を送信し、認証処理が完了する。セッションキーは、認証動作の度に異なる値となる。

ステップＳＴ１７における比較の結果が同一でない場合には、ドライブ１０２によるホスト１０３の認証が失敗したことになり、ステップＳＴ１９において、認証が失敗したことを示すエラー情報がホスト

１０３に送信される。

ホスト１０３は、送付したコマンドSEND KEYに対する応答としてドライブ１０２から認証が成功したか否かを示す情報を受け取り、受け取った情報に基づいてステップＳＴ２８において、認証完了か否かを判断する。認証が成功したことを示す情報を受け取ることで認証完了と判断し、認証が失敗したことを示す情報を受け取ることで認証が完了しなかったと判断する。認証が完了した場合は、ステップＳＴ２９において、ＭＡＣ演算ブロック１３５がドライブ側と共通のセッションキーeKm(Ra3‖Rb3)（例えば６４ビット長）を生成する。認証が完了しなかった場合には、リジェクト処理がなされる。セッションキーeKm(Ra3‖Rb3)を以下の説明では、適宜Ｋｓと表記する。

上述した一実施形態による相互認証は、ドライブ１０２がリボケーション機能を持つことができ、また、認証専用の特定の認証鍵を必要としない特徴を有している。

また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。

さらに、ドライブ１０２が比較１２９によってホスト１０３の認証結果を確認することで、ドライブ１０２がホスト１０３から正規のライセンスを受けた上で実装されたものであるか否かを判定することが可能となる。

次に、上述した相互認証を行うドライブ１０２とホスト１０３とを組み合わせて実現したレコーダの一実施形態の構成を第８図に示す。一実施形態のレコーダは、ドライブ１０２がメディアユニークキーを計算し、計算したメディアユニークキーを相互認証によって生成したセッションキーＫｓを用いてセキュアにホスト１０３に転送する。ま

た、ドライブ１０２がコンテンツキー導出のための乱数データを生成し、生成した乱数データを相互認証によって生成したセッションキーＫｓを用いてホスト１０３へセキュアに転送し、ホスト１０３が導出したコンテンツキーを用いてコンテンツを暗号化し、暗号化コンテンツをドライブ１０２へ転送し、ドライブ１０２が暗号化コンテンツをメディア１０１へ記録する構成とされている。

レコーダを構成するドライブ１０２は、デバイスキー１２１、プロセスＭＫＢ１２２、Ｃ２＿Ｇ２１４１、ＤＥＳ(Data Encryption Standard)エンクリプタ１４２、乱数発生器１４３、ＤＥＳエンクリプタ１４４の構成要素を有する。

メディア１０１から再生されたＭＫＢ１１２とデバイスキー１２１とがプロセスＭＫＢ１２２において演算されることによって、リボケーションされたかどうかの判別ができる。プロセスＭＫＢ１２２において、ＭＫＢ１１２とデバイスキー１２１からメディアキーが算出される。ＭＫＢ１１２の中にドライブ１０２のデバイスキー１２１が入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキー１２１を持つドライブ１０２が正当なものでないと判断され、ドライブ１０２がリボケーションされる。

Ｃ２＿Ｇ１４１は、メディアキーとメディアＩＤ１１１とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーがＤＥＳエンクリプタ１４２にてセッションキーＫｓによって暗号化される。暗号化の方式として、例えばＤＥＳ　ＣＢＣモードが使用される。ＤＥＳエンクリプタ１４２の出力がホスト１０３のＤＥＳデクリプタ１５１に送信される。

乱数発生器１４３によってタイトルキーが生成される。乱数発生器

１４３からのタイトルキーがＤＥＳエンクリプタ１４４に入力され、タイトルキーがセッションキーで暗号化される。暗号化タイトルキーがホスト１０３のＤＥＳデクリプタ１５２に送信される。

ホスト１０３において、ＤＥＳデクリプタ１５１において、セッションキーＫｓによってメディアユニークキーが復号される。ＤＥＳデクリプタ１５２において、セッションキーＫｓによってタイトルキーが復号される。メディアユニークキーおよびタイトルキーがＣ２＿Ｅ１５３に供給され、タイトルキーがメディアユニークキーを使用してＣ２によって暗号化される。暗号化タイトルキー１１４がメディア１０１に記録される。

ホスト１０３においては、ＣＣＩと復号されたタイトルキーとがＣ２＿Ｇ１５４に供給され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＥＣＢＣ１５５に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ１１３がメディア１０１に記録される。

第９図は、コンテンツ記録時の手順を示すものである。最初に、ホスト１０３からの要求に応じてメディア１０１上のＭＫＢがシークされ、読み出される（ステップＳ２１）。次のステップＳ２２のＡＫＥ(Authentication and Key Exchange)において、上述したようなリボーク処理とドライブ１０２とホスト１０３の相互認証動作がなされる。

相互認証動作は、電源のＯＮ後のディスク検出時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ１０２およびホスト１０３の両者において、セッションキーＫｓが生成され、セッションキーＫｓが共有される。

次のステップＳ２３において、ホスト１０３がドライブ１０２に対してメディアユニークキーを要求する。ドライブ１０２は、メディア１０１のメディアＩＤをシークし（ステップＳ２４）、メディアＩＤをメディア１０１から読み出す（ステップＳ２５）。ドライブ１０２は、メディアキーとメディアＩＤとを演算することによってメディアユニークキーを生成する。ステップＳ２６において、メディアユニークキーがセッションキーＫｓによって暗号化され、暗号化されたメディアユニークキーがホスト１０３に転送される。

次に、ステップＳ２７において、ホスト１０３がドライブ１０２に対してタイトルキーを要求する。ステップＳ２８において、ドライブ１０２がタイトルキーをセッションキーＫｓで暗号化し、暗号化したタイトルキーをホスト１０３に転送する。ホスト１０３において、セッションキーＫｓによって、暗号化されたメディアユニークキーおよび暗号化されたタイトルキーがそれぞれ復号される。

そして、タイトルキーがメディアユニークキーによって暗号化され、暗号化タイトルキーが生成される。また、タイトルキーとＣＣＩからコンテンツキーが生成され、コンテンツキーによってコンテンツが暗号化される。ステップＳ２９において、ホスト１０３からドライブ１０２に対して、暗号化タイトルキー、暗号化コンテンツおよびＣＣＩが転送される。ステップＳ３０において、ドライブ１０２によって、これらの暗号化タイトルキー、暗号化コンテンツおよびＣＣＩがメディア１０１に対して記録される。

なお、第８図のレコーダの構成においては、ドライブ１０２において乱数発生器１４３を使用してタイトルキーを生成している。しかしながら、ホスト１０３に乱数発生器を設け、この乱数発生器によってタイトルキーを生成するようにしても良い。

次に、上述した相互認証を行うドライブ１０２とホスト１０３とを組み合わせて実現したプレーヤの一実施形態の構成を第１０図に示す。一実施形態のプレーヤは、ドライブ１０２が計算したメディアユニークキーを相互認証によって生成したセッションキーＫｓを用いてセキュアにホスト１０３に転送し、ホスト１０３が暗号化タイトルキーをメディアユニークキーによって復号し、タイトルキーとＣＣＩとから導出したコンテンツキーを用いてコンテンツを復号する構成とされている。

プレーヤを構成するドライブ１０２は、デバイスキー１２１、プロセスＭＫＢ１２２、Ｃ２＿Ｇ２１４１、ＤＥＳエンクリプタ１４２の構成要素を有する。メディア１０１から再生されたＭＫＢ１１２とデバイスキー１２１とがプロセスＭＫＢ１２２において演算されることによって、リボケーションされたかどうかの判別ができる。プロセスＭＫＢ１２２において、ＭＫＢ１１２とデバイスキー１２１からメディアキーが算出される。

Ｃ２＿Ｇ１４１は、メディアキーとメディアＩＤ１１１とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーがＤＥＳエンクリプタ１４２にてセッションキーＫｓによって暗号化される。暗号化の方式として、例えばＤＥＳ　ＣＢＣモードが使用される。ＤＥＳエンクリプタ１４２の出力がホスト１０３のＤＥＳデクリプタ１５１に送信される。

ホスト１０３において、ＤＥＳデクリプタ１５１において、セッシ

ョンキーＫｓによってメディアユニークキーが復号される。メディアユニークキーおよび暗号化タイトルキー１１４がＣ２＿Ｄ１５３に供給され、暗号化タイトルキーがメディアユニークキーを使用して復号される。復号されたタイトルキーとメディア１０１から再生されたＣＣＩがＣ２＿Ｇ１５４に供給され、コンテンツキーが導出される。メディア１０１から再生された暗号化コンテンツ１１３がＣ２デクリプタ１５５において、コンテンツキーによって復号され、コンテンツが得られる。

第１１図は、コンテンツ再生時の手順を示すものである。最初に、ホスト１０３からの要求に応じてメディア１０１上のＭＫＢがシークされ、読み出される（ステップＳ４１）。ＭＫＢがパック毎に読み出される。次のステップＳ４２のＡＫＥにおいて、上述したようなリボーク処理とドライブ１０２とホスト１０３の相互認証動作がなされる。

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ１０２およびホスト１０３の両者において、セッションキーＫｓが生成され、セッションキーＫｓが共有される。

次のステップＳ４３において、ホスト１０３がドライブ１０２に対してメディアユニークキーを要求する。ドライブ１０２は、メディア１０１のメディアＩＤをシークし（ステップＳ４４）、メディアＩＤをメディア１０１から読み出す（ステップＳ４５）。ドライブ１０２は、メディアキーとメディアＩＤとを演算することによってメディアユニークキーを生成する。ステップＳ４６において、メディアユニークキーがセッションキーＫｓによって暗号化され、暗号化されたメディアユニークキーがホスト１０３に転送される。

次に、ステップＳ４７において、ホスト１０３がドライブ１０２に対して、暗号化タイトルキー、ＣＣＩおよび暗号化コンテンツを要求する。ステップＳ４８において、ドライブ１０２が暗号化タイトルキー１１４、ＣＣＩ１１５および暗号化コンテンツ１１３をメディア１０１からリードする。ステップＳ４９において、ドライブ１０２が暗号化タイトルキー１１４、ＣＣＩ１１５および暗号化コンテンツ１１３を読み取る。そして、ステップＳ５０において、ドライブ１０２が暗号化タイトルキー１１４、ＣＣＩ１１５および暗号化コンテンツ１１３をホスト１０３に対して転送する。

ホスト１０３において、タイトルキーが復号され、タイトルキーとＣＣＩとからコンテンツキーが求められ、コンテンツキーを鍵として暗号化コンテンツが復号される。

第１０図に示すプレーヤの構成においては、ホスト１０３が暗号化タイトルキーを復号するデクリプタＣ２＿Ｄ１５３を備えているが、ドライブ１０２が暗号化タイトルキーを復号するデクリプタを備えるようにしても良い。この場合、復号されたタイトルキーがホスト１０３のコンテンツキー生成用のＣ２＿Ｇ１５４に対してセキュアに転送される。または、ドライブ１０２にコンテンツキー生成装置Ｃ２＿Ｇを設け、ドライブ１０２において復号されたタイトルキーとＣＣＩとからコンテンツキーを生成するようにしても良い。この場合、復号されたコンテンツキーがホスト１０３のＣ２＿ＤＣＢＣ１５５へセキュアに転送される。

第１２図は、相互認証を行うドライブ１０２とホスト１０３とを組み合わせて実現したレコーダの他の実施形態の構成を示す。他の実施形態のレコーダは、ドライブ１０２が計算したメディアユニークキーを相互認証によって生成したセッションキーＫｓを用いてセキュアに

ホスト１０３に転送する。また、ドライブ１０２においてコンテンツキーが生成され、生成されたコンテンツキーがセッションキーＫｓを用いてホスト１０３へセキュアに転送され、ホスト１０３が復号したコンテンツキーを用いてコンテンツを暗号化し、暗号化コンテンツをドライブ１０２へ転送し、ドライブ１０２が暗号化コンテンツをメディア１０１へ記録する構成とされている。すなわち、第８図に示す上述したレコーダでは、ホスト１０３においてコンテンツキーを生成したが、他の実施形態では、ドライブ１０２において、コンテンツキーを生成している。

第１２図に示すように、メディア１０１から再生されたＭＫＢ１１２とデバイスキー１２１とがプロセスＭＫＢ１２２において演算されることによって、メディアキーが算出され、Ｃ２＿Ｇ１４１において、メディアキーとメディアＩＤ１１１とが演算し、メディアユニークキーが導出される。メディアユニークキーがＤＥＳエンクリプタ１４２にてセッションキーＫｓによって暗号化され、ＤＥＳエンクリプタ１４２の出力がホスト１０３のＤＥＳデクリプタ１５１に送信され、ＤＥＳデクリプタ１５１によってメディアユニークキーが導出される。

さらに、ドライブ１０２の乱数発生器１４３によってタイトルキーが生成され、乱数発生器１４３からのタイトルキーがホスト１０３のＣ２＿Ｅ１５３に供給され、タイトルキーがメディアユニークキーを使用してＣ２によって暗号化される。暗号化タイトルキー１１４がメディア１０１に記録される。

ホスト１０３において、セッションキーＫｓを鍵としてＭＡＣ演算ブロック１５８によりＣＣＩのＭＡＣ値ｅＫｓ（ＣＣＩ）が計算され、ＣＣＩとともにドライブ１０２へ転送される。

ドライブ１０２において、ホスト１０３から受け取ったＣＣＩからセッションキーＫｓを鍵としてＭＡＣ演算ブロック１５７によりＣＣＩのＭＡＣ値ｅＫｓ（ＣＣＩ）が計算され、ホスト１０３から受け取ったＭＡＣ値とともに比較１５９へ供給される。

比較１５９では、両方のＭＡＣ値が一致したならば、ホスト１０３から受け取ったＣＣＩの改ざんは無いものと判断し、スイッチＳＷ２をＯＮする。一致しなかった場合は、ＣＣＩは改ざんされたものとみなし、スイッチＳＷ２をＯＦＦし、以降の処理を中断する。

ドライブ１０２において、ホスト１０３から受け取ったＣＣＩとタイトルキーとがＣ２＿Ｇ１４５に供給され、コンテンツキーが導出される。コンテンツキーがＤＥＳエンクリプタ１４６に供給され、セッションキーＫｓを鍵として、コンテンツキーが暗号化される。暗号化コンテンツキーがホスト１０３のＤＥＳデクリプタ１５６に転送される。

ＤＥＳデクリプタ１５６でセッションキーＫｓを鍵として復号されたコンテンツキーがＣ２＿ＥＣＢＣ１５５に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ１１３がドライブ１０２に転送され、ドライブ１０２によってメディア１０１に記録される。

なお、第１２図に示すレコーダにおいては、タイトルキーがドライブ１０２の乱数発生器１４３によって生成されている。しかしながら、ホスト１０３側に乱数発生器を設け、この乱数発生器によってタイトルキーを生成しても良い。この場合には、生成されたタイトルキーがホスト１０３からドライブ１０２のコンテンツキー生成のためのＣ２＿Ｇ１４５に対して転送される。

第１３図は、レコーダの他の実施形態によるコンテンツ記録時の手

順を示すものである。最初に、ホスト１０３からの要求に応じてメディア１０１上のＭＫＢがシークされ、読み出される（ステップＳ６１）。次のステップＳ６２のＡＫＥにおいて、リボーク処理とドライブ１０２とホスト１０３の相互認証動作がなされる。

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ１０２およびホスト１０３の両者において、セッションキーＫｓが生成され、セッションキーＫｓが共有される。

次のステップＳ６３において、ホスト１０３がドライブ１０２に対してメディアユニークキーを要求する。ドライブ１０２は、メディア１０１のメディアＩＤをシークし（ステップＳ６４）、メディアＩＤをメディア１０１から読み出す（ステップＳ６５）。ドライブ１０２は、メディアキーとメディアＩＤとを演算することによってメディアユニークキーを生成する。ステップＳ６６において、メディアユニークキーがセッションキーＫｓによって暗号化され、暗号化されたメディアユニークキーがホスト１０３に転送される。

次に、ステップＳ６７において、ホスト１０３がドライブ１０２に対してタイトルキーを要求する。ステップＳ６８において、ドライブ１０２がタイトルキーをホスト１０３に転送する。ホスト１０３において、セッションキーＫｓによって、暗号化されたメディアユニークキーが復号される。そして、タイトルキーがメディアユニークキーによって暗号化され、暗号化タイトルキーが生成される。

また、ステップＳ６９において、ホスト１０３がドライブ１０２に対してＣＣＩを送る。このとき、ＣＣＩの改ざんを回避するためにＣＣＩの認証データとして計算されたＭＡＣ値ｅＫｓ（ＣＣＩ）を付加して転送する。ドライブ１０２において、ＣＣＩの改ざんが無いこと

を確認後、タイトルキーとＣＣＩからコンテンツキーが生成され、コンテンツキーがセッションキーＫｓで暗号化される。ステップＳ７０において、ホスト１０３がドライブ１０２に対してコンテンツキーを要求すると、ステップＳ７１において、ドライブ１０２が暗号化されたコンテンツキーをホスト１０３に送る。

ホスト１０３は、暗号化コンテンツキーをセッションキーＫｓによって復号し、コンテンツキーを得る。コンテンツキーによってコンテンツが暗号化される。ステップＳ７２において、ホスト１０３からドライブ１０２に対して、暗号化タイトルキー、暗号化コンテンツおよびＣＣＩが転送される。ステップＳ７３において、ドライブ１０２によって、暗号化タイトルキー、暗号化コンテンツおよびＣＣＩがメディア１０１に対して記録される。

上述した第１２図に示す構成のレコーダは、ドライブ１０２において、真正乱数またはそれに近い乱数をハードウェア例えばＬＳＩによって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。また、ドライブ１０２において、ハードウェア構成によってコンテンツキーを生成するので、著作権保護の実装を強力とすることができる。

この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばタイトルキーは、タイトル毎のキーであるが、この発明では、乱数情報であれば、タイトル毎に異なることは、必要ではない。

また、上述した説明においては、著作権保護技術としてＣＰＲＭおよびＣＰＲＭを拡張した例を挙げたが、ＣＰＲＭ以外の著作権保護技術に対してもこの発明を適用することができる。例えば、特開2001－

352322号公報において提案されるツリー構造の鍵配布構成に基づく著作権保護技術に対して適用可能である。また、ＰＣベースのシステムに対してこの発明が適用されるが、このことは、ＰＣとドライブを組み合わせる構成にのみ限定されることを意味するものではない。例えば携帯型動画または静止画カメラの場合に、メディアとして光ディスクを使用し、メディアを駆動するドライブとドライブを制御するマイクロコンピュータが設けられる動画または静止画カメラシステムに対してもこの発明を適用することが可能である。

この発明では、メディア上に記録された鍵情報（ＭＫＢ）と各デバイスまたは各アプリケーションに記憶されている鍵情報（デバイスキー）から同一の値として導かれる鍵情報（メディアキー）を利用して相互認証がなされる。したがって、この発明においては、認証のためだけに用意される特定の認証鍵を必要とせず、秘密情報を少なくでき、また、デバイスまたはアプリケーションによってデバイスキーを異ならせることが可能であるので、秘密情報が不正に読み取られる危険性を少なくできる。

この発明では、著作権保護技術に関する秘密情報である電子機器またはアプリケーションソフトウェア固有の情報例えばデバイスキーがドライブ内に実装されているので、情報処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持たせることが容易に実施でき、また、ディスクからのデータとしてそのまま読み出された暗号化コンテンツが「ＤｅＣＳＳ」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を防ぐことができること

から、著作権保護技術の安全性を確保することができる。

また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。

さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばＬＳＩによって生成できるので、ＰＣ内でソフトウェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少なくできる。

請 求 の 範 囲

1．不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法において、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第1の判定ステップを有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定ステップを有し、

上記第1の判定ステップによって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、上記第2の判定ステップによって無効化すべきという判定をされなかった場合に生成される第2の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法。

2．請求の範囲第1項において、

上記相互認証ステップは、

上記情報処理装置が上記伝達手段を介して正常に動作しているかを上記再生装置において確認する第1の確認ステップと、

上記再生装置が上記伝達手段を介して正常に動作しているかを上記情報処理装置において確認する第2の確認ステップとを有することを特徴とする請求の範囲第1項に記載の相互認証方法。

3． 請求の範囲第2項において、

上記再生装置は、

乱数を生成する第1の乱数生成ステップと、

所定の計算をする第1の計算ステップとを有し、

上記情報処理装置は、

乱数を生成する第2の乱数生成ステップと、

所定の計算をする第2の計算ステップとを有し、

上記第1の確認ステップは、

上記第1の乱数生成ステップにより生成される第1の乱数と、上記第2の乱数生成ステップにより生成される第2の乱数とを上記伝達手段を介して上記再生装置と上記情報処理装置との間で相互に交換する第1の乱数交換ステップと、

上記再生装置において、少なくとも上記第1の鍵情報と上記相互に交換された第1の乱数および第2の乱数とを用いて上記第1の計算ステップにより計算した結果と、上記情報処理装置から上記伝達手段を介して送られた、少なくとも上記第2の鍵情報と上記相互に交換された第1の乱数および第2の乱数とを用いて上記第2の計算ステップにより計算した結果とが同一であるかを比較する第1の比較ステップとを有し、

上記第2の確認ステップは、

上記第1の乱数生成ステップにより生成される第3の乱数と、上記第2の乱数生成ステップにより生成される第4の乱数とを上記伝達手段を介して上記再生装置および上記情報処理装置との間で相互に交換する第2の乱数交換ステップと、

上記情報処理装置において、上記再生装置から上記伝達手段を介して送られた、少なくとも上記第1の鍵情報と上記相互に交換された第3の乱数および第4の乱数とを用いて上記第1の計算ステップにより

計算した結果と、少なくとも上記第２の鍵情報と上記相互に交換された第３の乱数および第４の乱数とを用いて上記第２の計算ステップにより計算した結果とが同一であるかを比較する第２の比較ステップとを有していることを特徴とする相互認証方法。

４．不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムであって、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第１の判定ステップを有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定ステップを有し、

上記第１の判定ステップによって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、上記第２の判定ステップによって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプログラム。

５．不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムを格納した記録媒体であって、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第1の判定ステップを有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定ステップを有し、

上記第1の判定ステップによって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、上記第2の判定ステップによって無効化すべきという判定をされなかった場合に生成される第2の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプログラムを格納した記録媒体。

6．不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置とを備える信号処理システムであって、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第1の判定手段を有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定手段を有し、

上記第1の判定手段によって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、上記第2の判定手段によって無効化すべきという判定をされなかった場合に生成される第2の鍵情報

とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証手段と、

上記相互認証手段による相互認証後に、上記再生装置および上記情報処理装置に共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする信号処理システム。

7．請求の範囲第6項において、

上記相互認証手段は、

上記情報処理装置が上記伝達手段を介して正常に動作しているかを上記再生装置において確認する第1の確認手段と、

上記再生装置が上記伝達手段を介して正常に動作しているかを上記情報処理装置において確認する第2の確認手段とを有することを特徴とする信号処理システム。

8．請求の範囲第7項において、

上記再生装置は、

乱数を生成する第1の乱数生成手段と、

所定の計算をする第1の計算手段とを有し、

上記情報処理装置は、

乱数を生成する第2の乱数生成手段と、

所定の計算をする第2の計算手段とを有し、

上記第1の確認手段は、

上記第1の乱数生成手段により生成される第1の乱数と、上記第2の乱数生成手段により生成される第2の乱数とを上記伝達手段を介して上記再生装置と上記情報処理装置との間で相互に交換する第1の乱数交換手段と、

上記再生装置において、少なくとも上記第1の鍵情報と上記相互に交換された第1の乱数および第2の乱数とを用いて上記第1の計算手

段により計算した結果と、上記情報処理装置から上記伝達手段を介して送られた、少なくとも上記第2の鍵情報と上記相互に交換された第1の乱数および第2の乱数とを用いて上記第2の計算手段により計算した結果とが同一であるかを比較する第1の比較手段とを有し、

上記第2の確認手段は、

上記第1の乱数生成手段により生成される第3の乱数と、上記第2の乱数生成手段により生成される第4の乱数とを上記伝達手段を介して上記再生装置および上記情報処理装置との間で相互に交換する第2の乱数交換手段と、

上記情報処理装置において、上記再生装置から上記伝達手段を介して送られた、少なくとも上記第1の鍵情報と上記相互に交換された第3の乱数および第4の乱数とを用いて上記第1の計算手段により計算した結果と、少なくとも上記第2の鍵情報と上記相互に交換された第3の乱数および第4の乱数とを用いて上記第2の計算手段により計算した結果とが同一であるかを比較する第2の比較手段とを有していることを特徴とする信号処理システム。

9．請求の範囲第8項において、

上記共通鍵生成手段は、

上記第1の乱数生成手段により生成される第5の乱数と、上記第2の乱数生成手段により生成される第6の乱数とを上記伝達手段を介して上記再生装置と上記情報処理装置との間で相互に交換する第3の乱数交換手段と、

上記再生装置において、少なくとも上記第1の鍵情報と上記第5の乱数と上記第6の乱数とを用いて上記共通鍵を生成する第1の共通鍵生成手段と、

上記情報処理装置において、少なくとも上記第2の鍵情報と上記第

5の乱数と上記第6の乱数とを用いて上記共通鍵を生成する第2の共通鍵生成手段とを有することを特徴とする信号処理システム。

１０．請求の範囲第9項において、

上記伝達手段を介して、上記共通鍵を用いた共通鍵暗号方式で上記再生装置から上記情報処理装置へ情報を送る第1の送信手段と、

上記再生装置において、上記第1の鍵情報と上記記録媒体固有の情報を用いて記録媒体固有の鍵情報を生成する中間鍵情報生成手段とを備えることを特徴とする請求の範囲第7項に記載の信号処理システム。

１１．請求の範囲第１０項において、

第3の鍵情報を、少なくとも上記記録媒体固有の鍵情報を用いて暗号化する鍵情報暗号化手段と、

上記鍵情報暗号化手段により暗号化された上記第3の鍵情報を上記記録媒体に記録する暗号化鍵情報記録手段と、

上記第3の鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、

上記コンテンツ情報暗号化鍵を用いて暗号化されたコンテンツ情報を上記記録媒体に記録するコンテンツ情報記録手段とを備えることを特徴とする信号処理システム。

１２．請求の範囲第１１項において、

上記鍵情報暗号化手段、上記暗号化鍵情報記録手段、上記最終暗号化鍵生成手段、上記コンテンツ情報記録手段は、

上記情報処理装置が有しているとともに、

上記記録媒体固有の鍵情報は、

上記第1の送信手段により上記情報処理装置へ送られることを特徴とする信号処理システム。

１３．請求の範囲第１２項において、

上記第３の鍵情報は、

上記再生装置において前期第１の乱数生成手段により生成された第７の乱数に基づいた鍵情報であるとともに、

当該第３の鍵情報は、

上記第１の送信手段により上記情報処理装置に送られることを特徴とする信号処理システム。

１４．請求の範囲第１２項において、

上記第３の鍵情報は、

上記情報処理装置において上記第２の乱数生成手段により生成された第８の乱数に基づいた鍵情報であることを特徴とする信号処理システム。

１５．請求の範囲第１１項において、

上記鍵情報暗号化手段、上記暗号化鍵情報記録手段、上記コンテンツ情報記録手段は、

上記情報処理装置が有しており、

上記記録媒体固有の鍵情報は、

上記第１の送信手段により上記情報処理装置へ送られるとともに、

上記最終暗号化鍵生成手段は、

上記再生装置が有しており、

上記最終暗号化鍵生成手段により生成された上記コンテンツ情報暗号化鍵は、

上記第１の送信手段により上記情報処理装置へ送られることを特徴とする信号処理システム。

１６．請求の範囲第１５項において、

上記第３の鍵情報は、

上記再生装置において上記第１の乱数生成手段により生成された第９の乱数を基にした鍵情報であることを特徴とする請求の範囲第１３項に記載の信号処理システム。

１７．請求の範囲第１５項において、

上記第３の鍵情報は、

上記情報処理装置において上記第２の乱数生成手段により生成された第１０の乱数を基にした鍵情報であるとともに、

上記伝達手段を介して、上記共通鍵を用いた共通鍵暗号方式で上記情報処理装置から上記再生装置へ情報を送る第２の送信手段により上記再生装置の上記最終暗号化鍵生成手段に送られることを特徴とする信号処理システム。

１８．請求の範囲第１０項において、

上記記録媒体から読み出される暗号化された第４の鍵情報を、少なくとも上記記録媒体固有の鍵情報を用いて復号する鍵情報復号手段と、

上記第４の鍵情報に基づいてコンテンツ情報復号鍵を生成する最終復号鍵生成手段と、

上記コンテンツ情報復号鍵を用いて上記コンテンツ情報を復号するコンテンツ情報復号手段とを備えていることを特徴とする信号処理システム。

１９．請求の範囲第１８項において、

上記最終復号鍵生成手段、上記コンテンツ情報復号手段は、

上記情報処理装置が有していることを特徴とする信号処理システム。

２０．請求の範囲第１９項において、

上記鍵情報復号手段は、

上記情報処理装置が有しており、

上記記録媒体固有の鍵情報は、

上記第１の送信手段によって上記情報処理装置へ送られることを特徴とする信号処理システム。

２１．請求の範囲第１９項において、

上記鍵情報復号手段は、

上記再生装置が有しており、

復号された上記第４の鍵情報は、

上記第１の送信手段によって上記情報処理装置へ送られることを特徴とする信号処理システム。

２２．請求の範囲第１８項において、

上記最終復号鍵生成手段は、

上記再生装置が有していることを特徴とする信号処理システム。

２３．請求の範囲第２２項において、

上記鍵情報復号手段は、

上記再生装置が有しており、

上記再生装置において生成された上記コンテンツ情報復号鍵は、

上記第１の送信手段によって上記情報処理装置へ送られることを特徴とする信号処理システム。

２４．不正な電子機器を判別するためのリボケーション情報記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有し、上記コンテンツ情報が伝達手段を介して情報処理装置に送信され、処理される信号処理システムにおける再生装置であって、

当該再生装置を表す情報と上記リボケーション情報とを用いて当該

再生装置を無効化すべきか否かを判定する第１の判定手段を有し、

上記第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、

上記情報処理装置に設けられている当該情報処理装置を表す情報と上記リボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、上記情報処理装置と相互に認証する相互認証手段と、

上記相互認証手段による相互認証後に、上記情報処理装置と共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする再生装置。

２５．不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、再生装置がコンテンツ情報を読み出し、上記コンテンツ情報が伝達手段を介して受信され、処理される情報処理装置であって、

上記再生装置に設けられている第１の判定手段によって、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定し、上記第１の判定手段によって無効化すべきという判定をされなかった場合に生成される第１の鍵情報と、

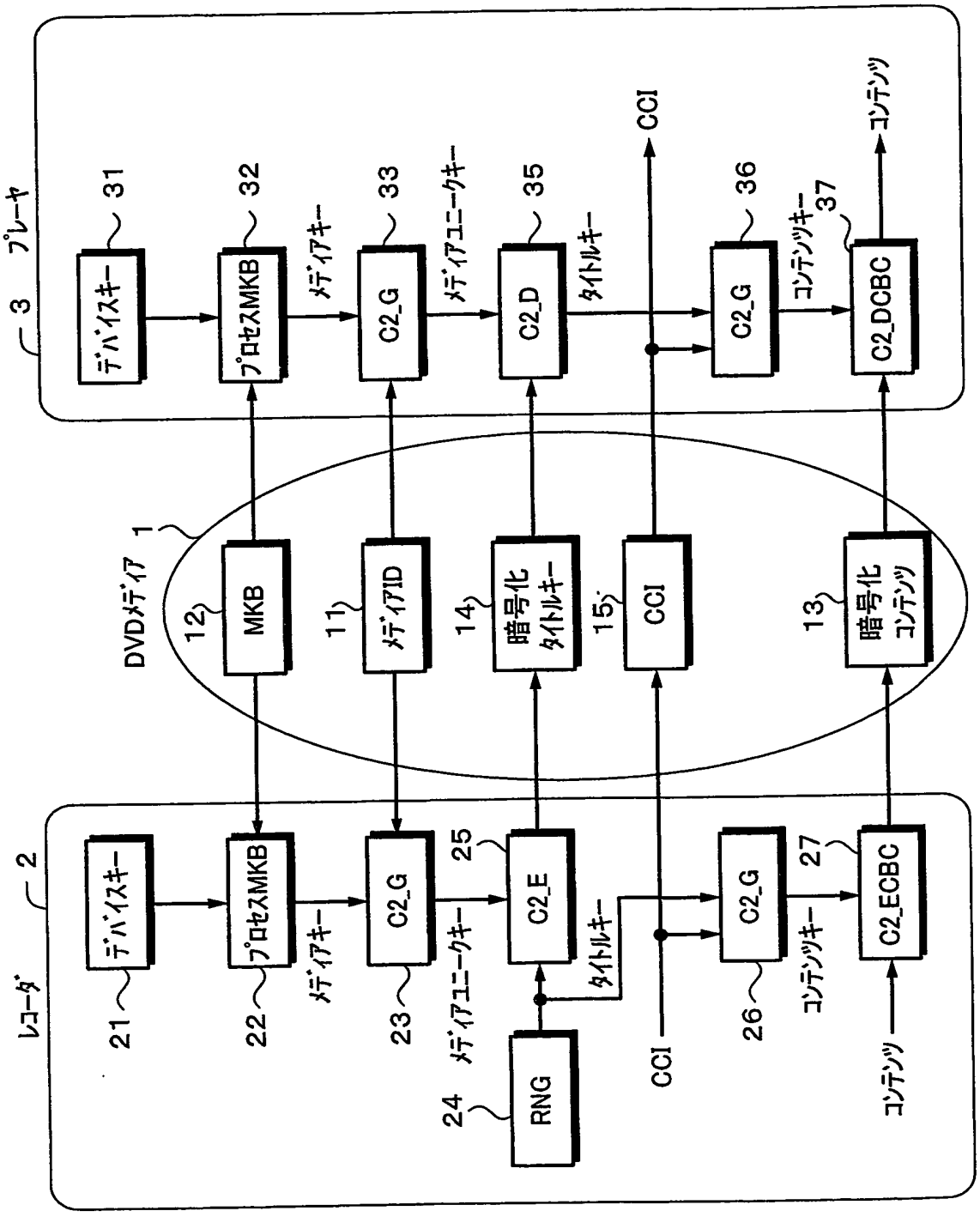
当該情報処理装置を表す情報と上記リボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第２の判定手段を有し、

上記第１の鍵情報と、上記第２の判定手段によって無効化すべきという判定をされなかった場合に生成される第２の鍵情報とを用いて、上記再生装置と相互に認証する相互認証手段と、

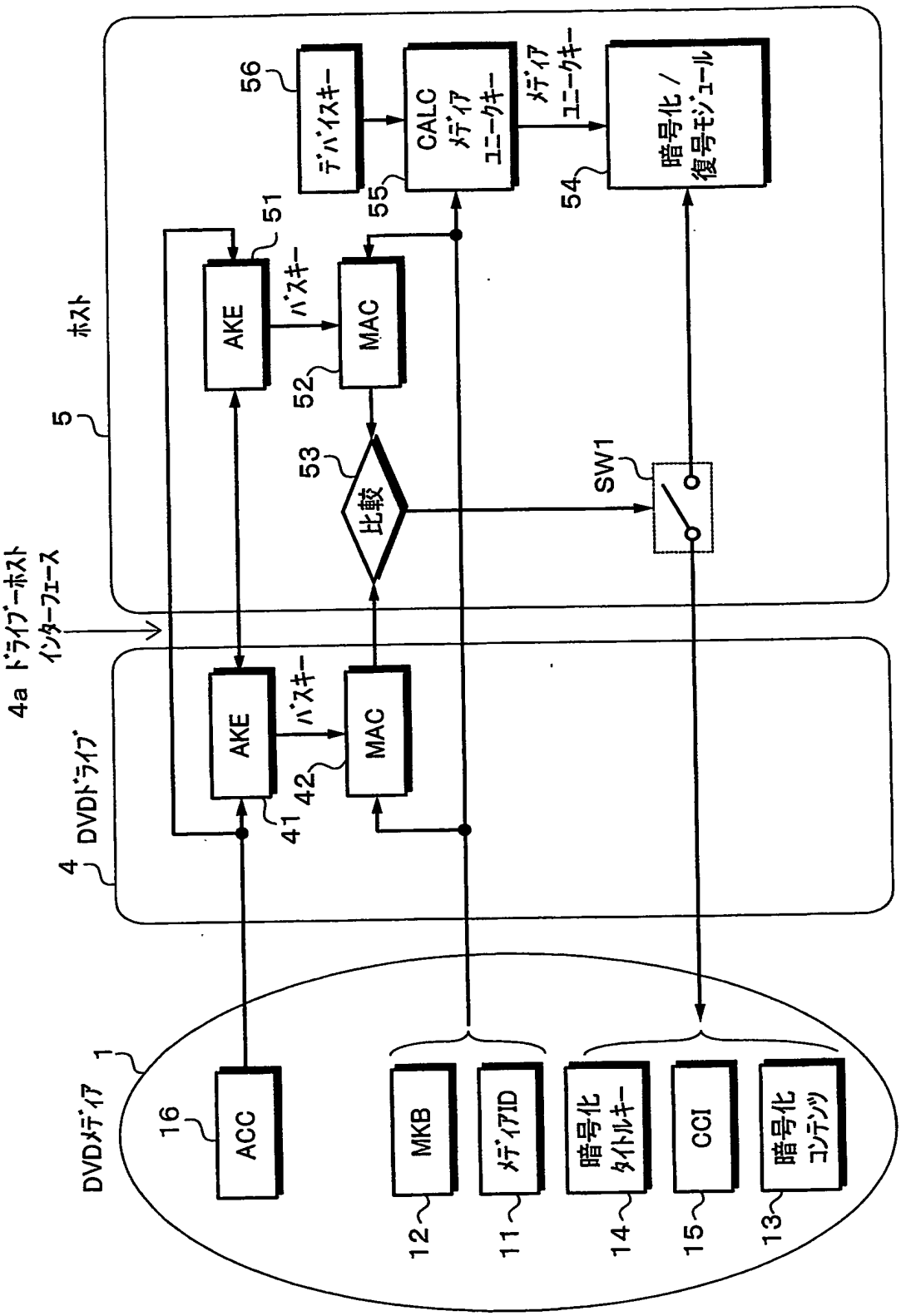
上記相互認証手段による相互認証後に、上記再生装置と共通の共通

鍵を生成する共通鍵生成手段とを備えることを特徴とする情報処理装置。

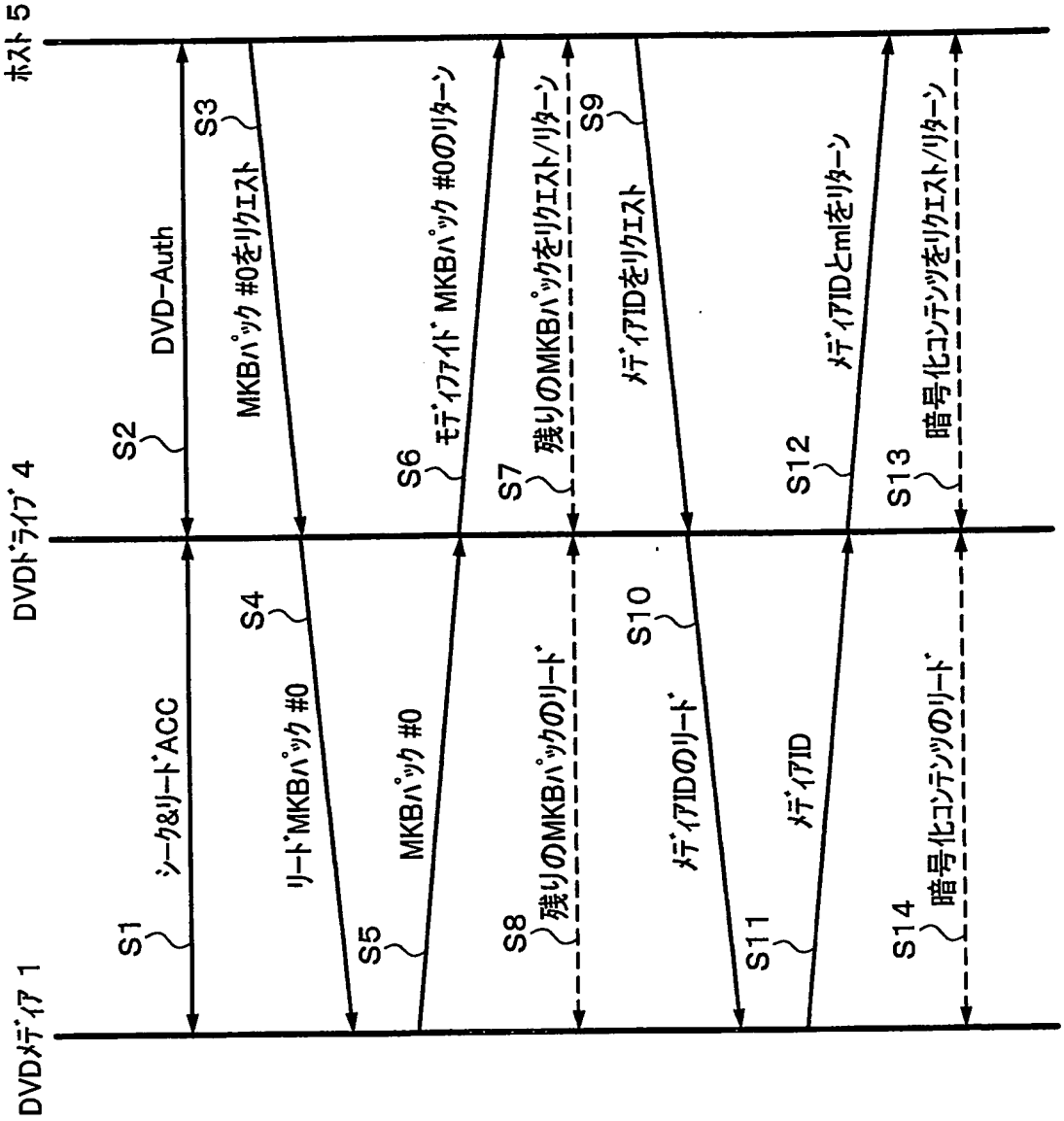
第１図


プレーヤ
3
デバイスキー
31
プロセスMKB
32
メディアキー
C2_G
33
メディアユニークキー
C2_D
35
タイトルキー
CCI
C2_G
36
コンテンツキー
37
C2_DCBC
コンテンツ
DVDメディア
1
MKB
12
メディアID
11
暗号化タイトルキー
14
CCI
15
暗号化コンテンツ
13
レコーダ
2
デバイスキー
21
プロセスMKB
22
メディアキー
C2_G
23
メディアユニークキー
C2_E
25
タイトルキー
RNG
24
CCI
C2_G
26
コンテンツキー
27
C2_ECBC
コンテンツ

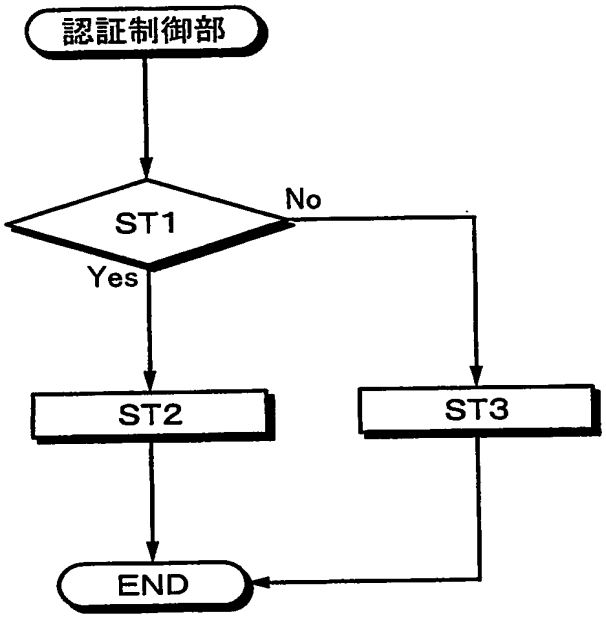
第２図


DVDメディア
1
16
ACC
MKB
12
メディアID
11
暗号化タイトルキー
14
CCI
15
暗号化コンテンツ
13
4
DVDドライブ
41
AKE
バスキー
42
MAC
4a ドライブ－ホスト インターフェース
5
ホスト
AKE
バスキー
51
MAC
52
53
比較
SW1
56
デバイスキー
CALC メディア ユニークキー
55
メディア ユニークキー
暗号化／復号モジュール
54

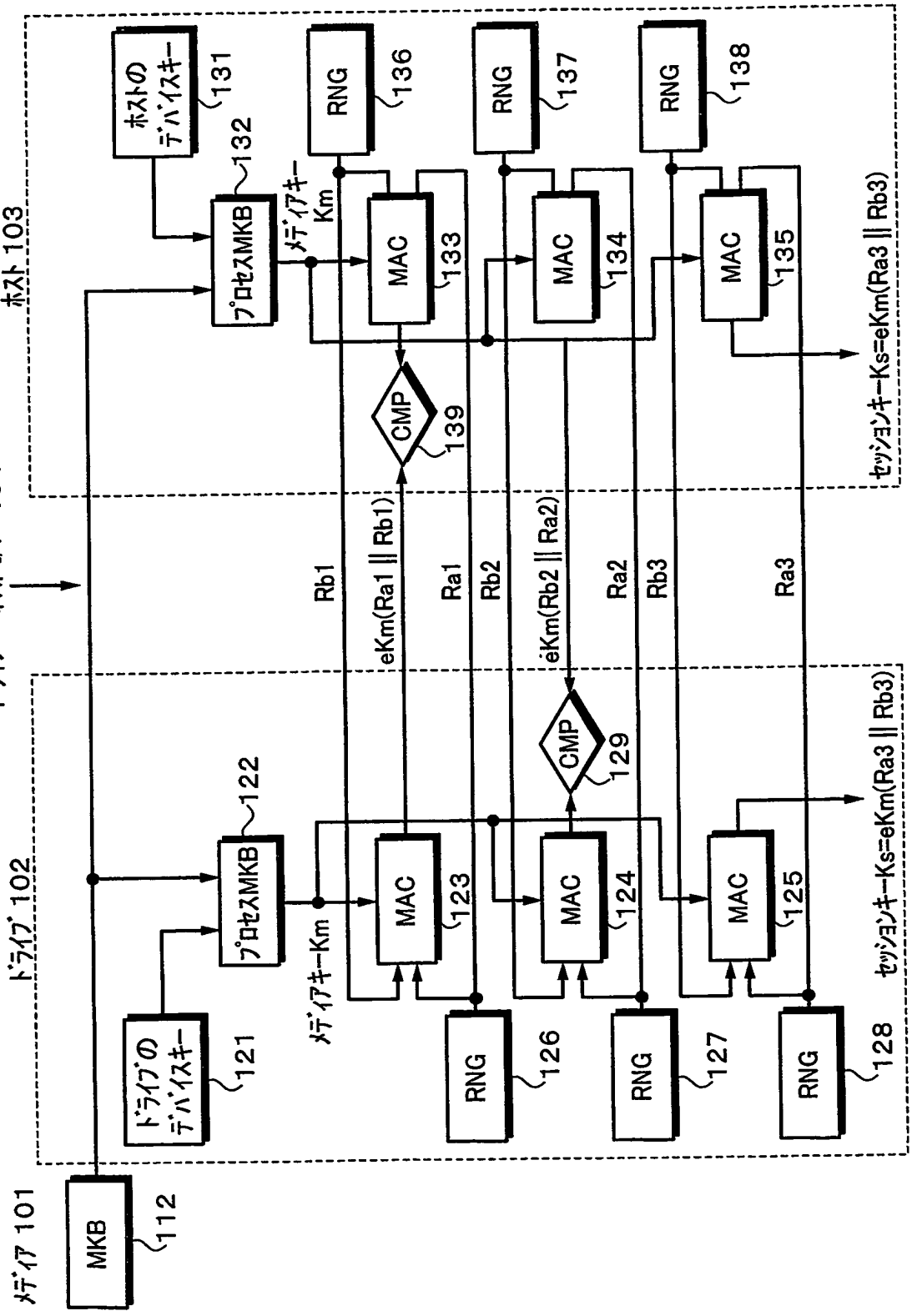
第３図


ホスト 5
DVDドライブ 4
DVDメディア 1
S1
シーク&リード'ACC
S2
DVD-Auth
S3
MKBパック #0をリクエスト
S4
リード'MKBパック #0
S5
MKBパック #0
S6
モデ'イファイド' MKBパック #0のリターン
S7
残りのMKBパックをリクエスト/リターン
S8
残りのMKBパックのリード'
S9
メデ'イアIDをリクエスト
S10
メデ'イアIDのリード'
S11
メデ'イアID
S12
メデ'イアIDとmlをリターン
S13
暗号化コンテンツをリクエスト/リターン
S14
暗号化コンテンツのリード'

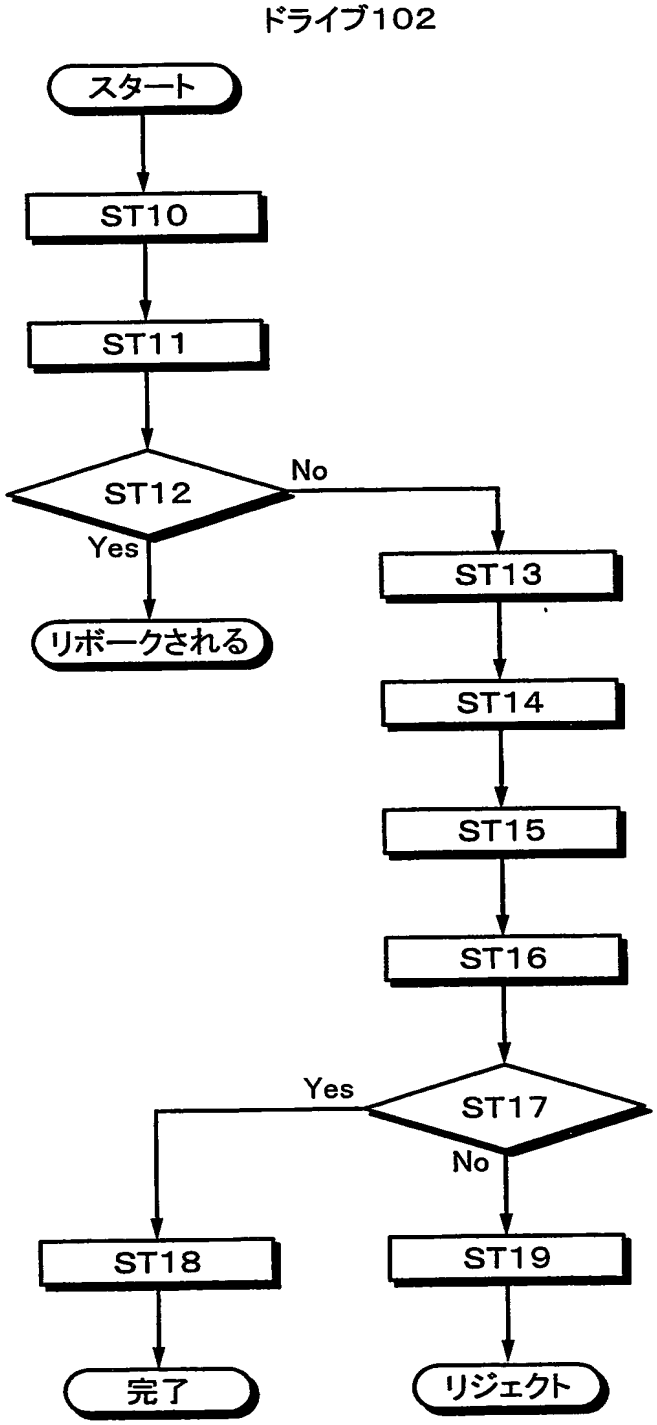
第４図



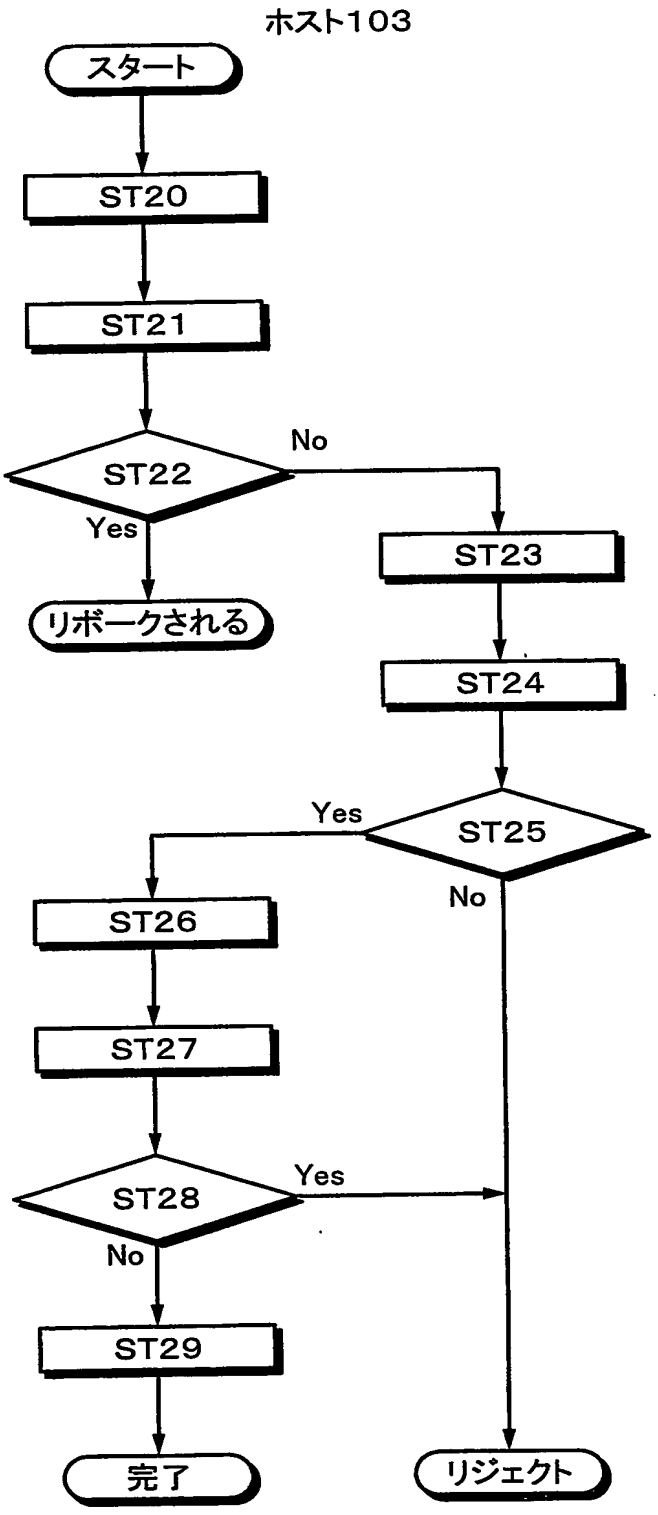
第5図


メディア 101
MKB
112
ドライブ 102
ドライブのデバイスキー
121
プロセスMKB
122
メディアキーKm
MAC
123
MAC
124
MAC
125
RNG
126
RNG
127
RNG
128
CMP
129
ドライブ - ホスト I/F 104
Rb1
eKm(Ra1 || Rb1)
Ra1
Rb2
eKm(Rb2 || Ra2)
Ra2
Rb3
Ra3
セッションキーKs=eKm(Ra3 || Rb3)
ホスト 103
ホストのデバイスキー
131
プロセスMKB
132
メディアキーKm
MAC
133
MAC
134
MAC
135
RNG
136
RNG
137
RNG
138
CMP
139
セッションキーKs=eKm(Ra3 || Rb3)

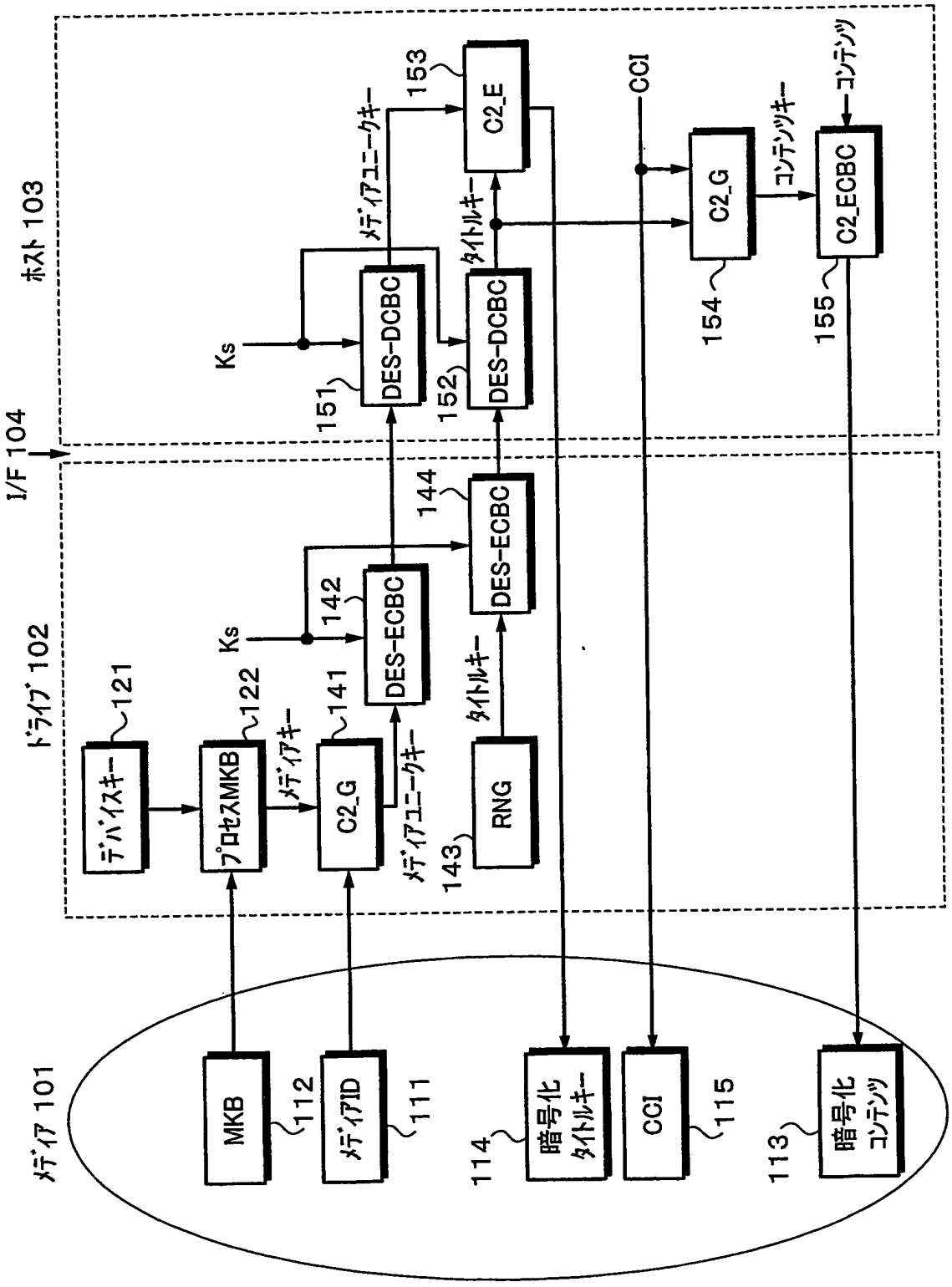
第６図


ドライブ102
スタート
ST10
ST11
ST12
No
Yes
リボークされる
ST13
ST14
ST15
ST16
ST17
Yes
No
ST18
ST19
完了
リジェクト

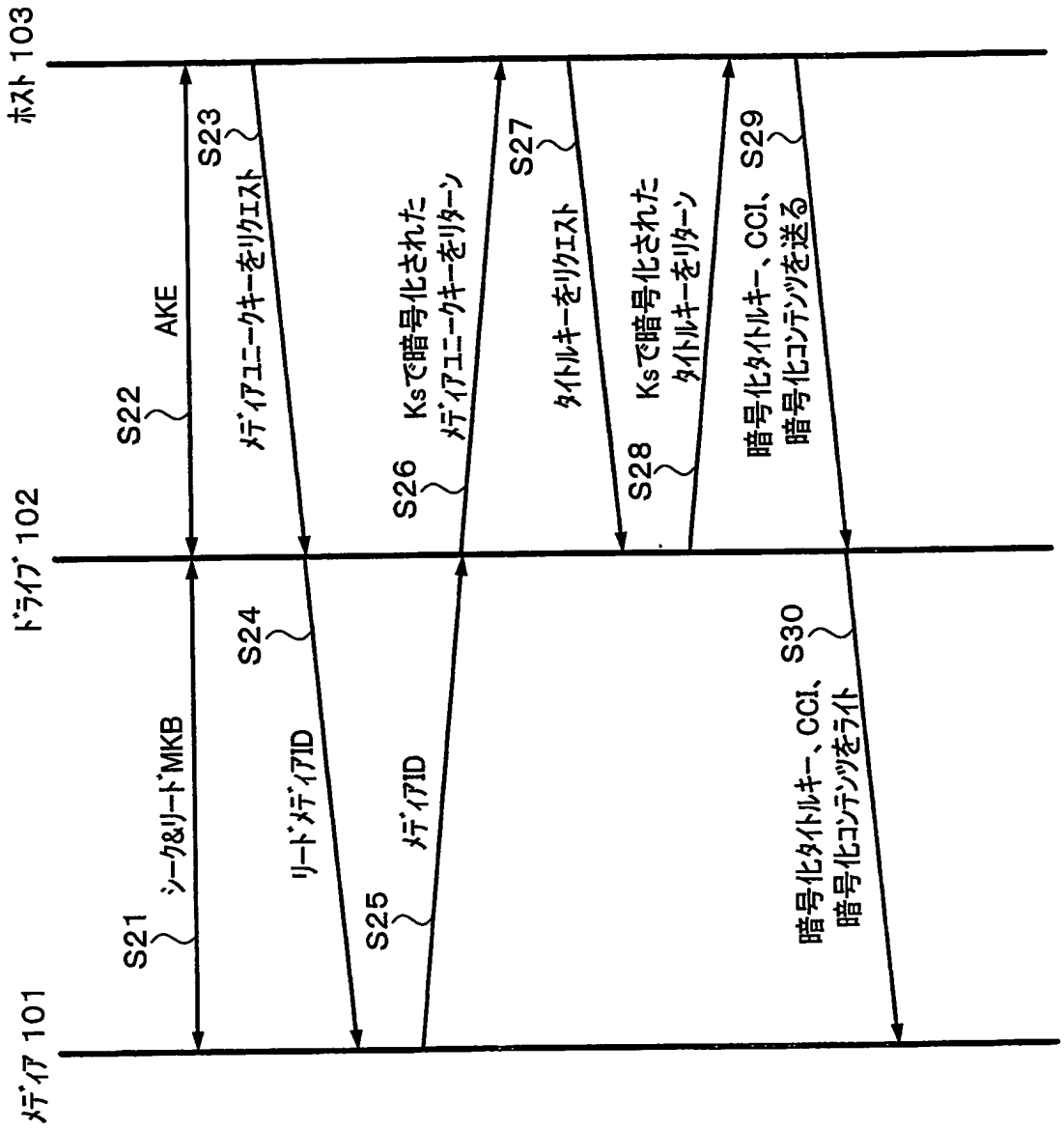
第７図


ホスト103
スタート
ST20
ST21
ST22
No
Yes
リボークされる
ST23
ST24
ST25
Yes
No
ST26
ST27
ST28
Yes
No
ST29
完了
リジェクト

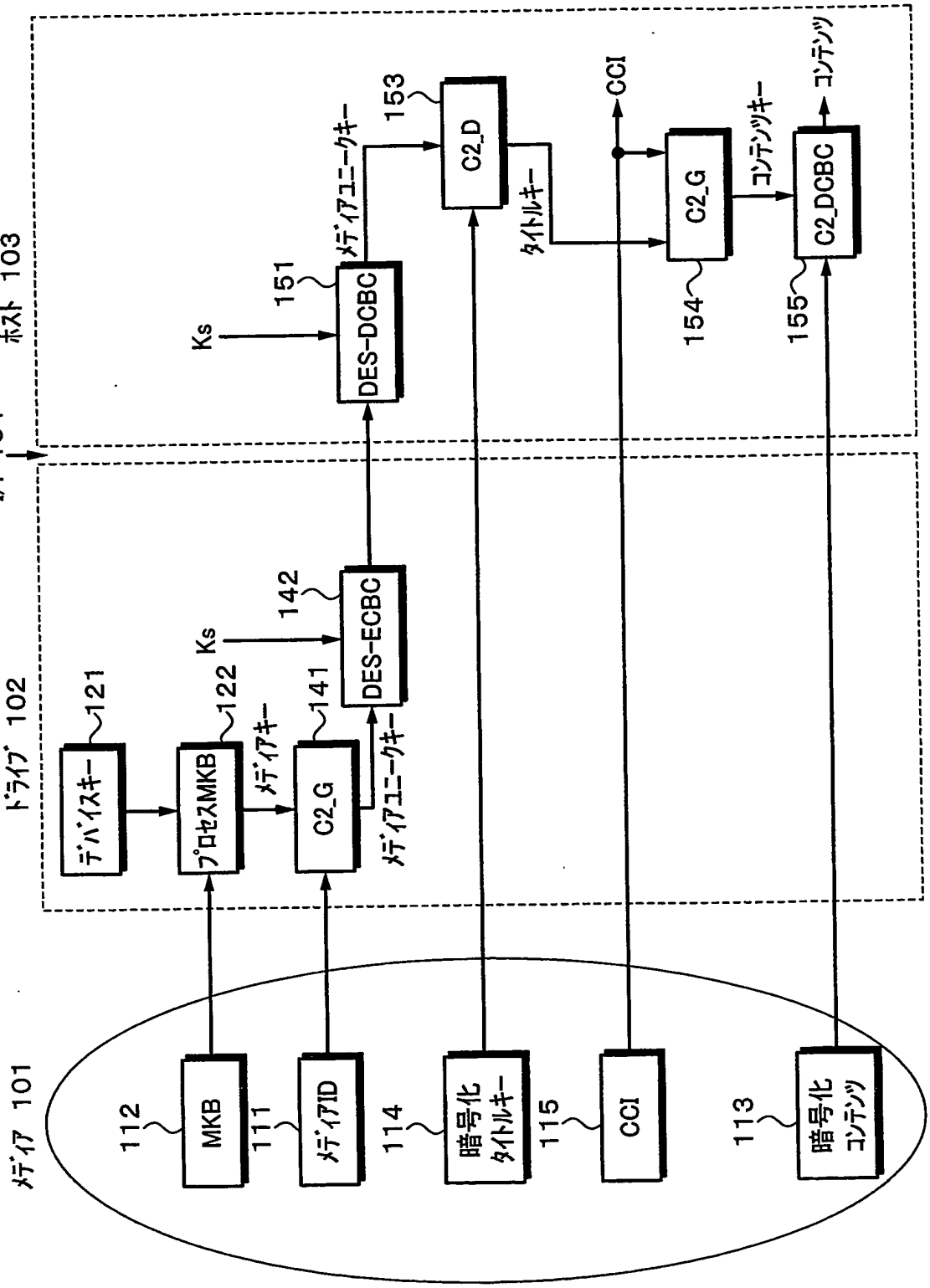
第８図


メディア 101
MKB
112
メディアID
111
暗号化タイトルキー
114
CCI
115
暗号化コンテンツ
113
I/F 104
ホスト 103
ドライブ 102
デバイスキー
121
プロセスMKB
122
メディアキー
C2_G
141
メディアユニークキー
DES-ECBC
142
Ks
RNG
143
タイトルキー
DES-ECBC
144
DES-DCBC
151
DES-DCBC
152
メディアユニークキー
C2_E
153
CCI
C2_G
154
コンテンツキー
C2_ECBC
155
コンテンツ

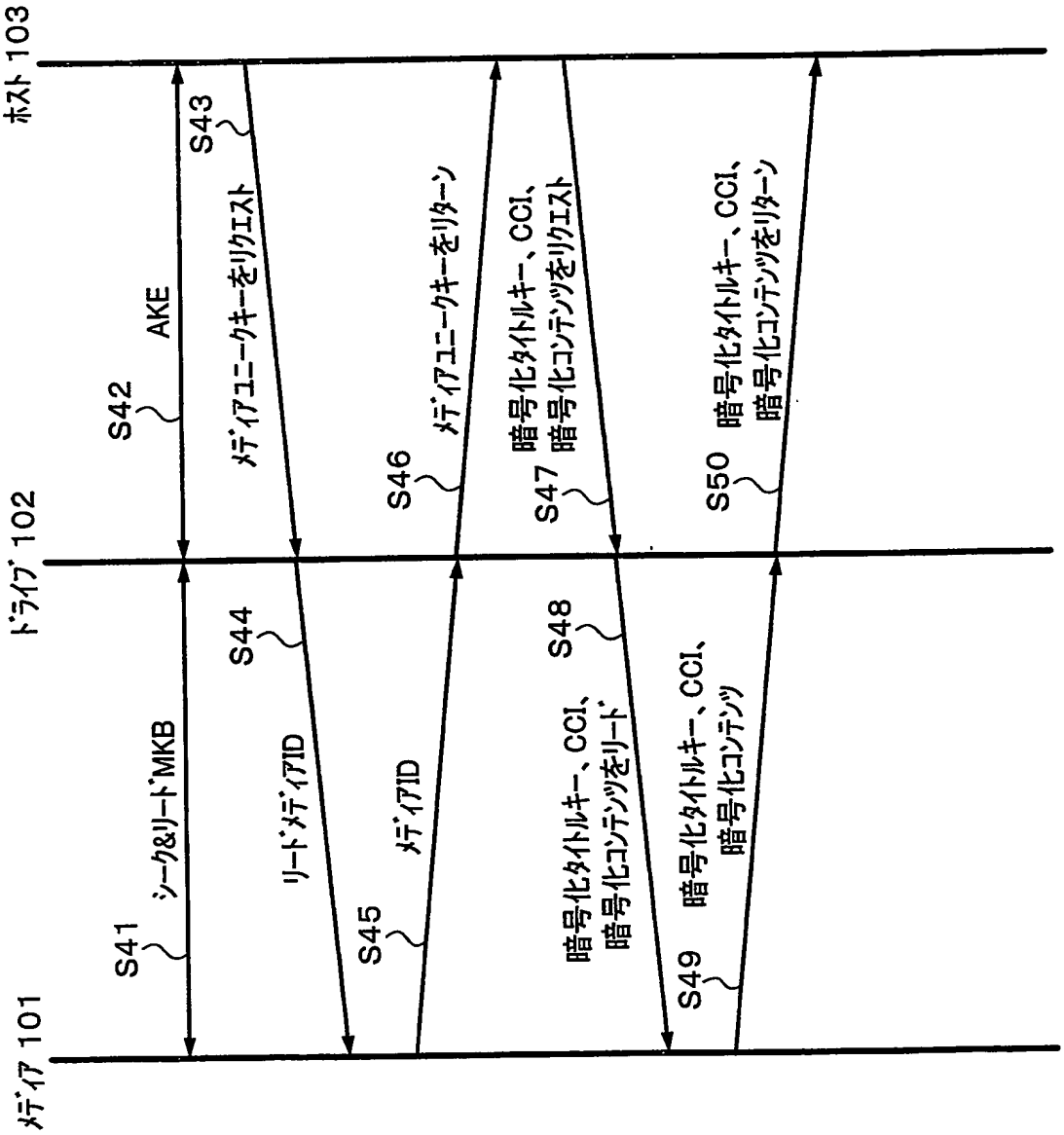
第9図


ホスト 103
ドライブ 102
メディア 101
S21
シーク&リード'MKB
S22
AKE
S23
メディアユニークキーをリクエスト
S24
リード'メディアID
S25
メディアID
S26
Ksで暗号化された
メディアユニークキーをリターン
S27
タイトルキーをリクエスト
S28
Ksで暗号化された
タイトルキーをリターン
S29
暗号化タイトルキー、CCI、
暗号化コンテンツを送る
S30
暗号化タイトルキー、CCI、
暗号化コンテンツをライト

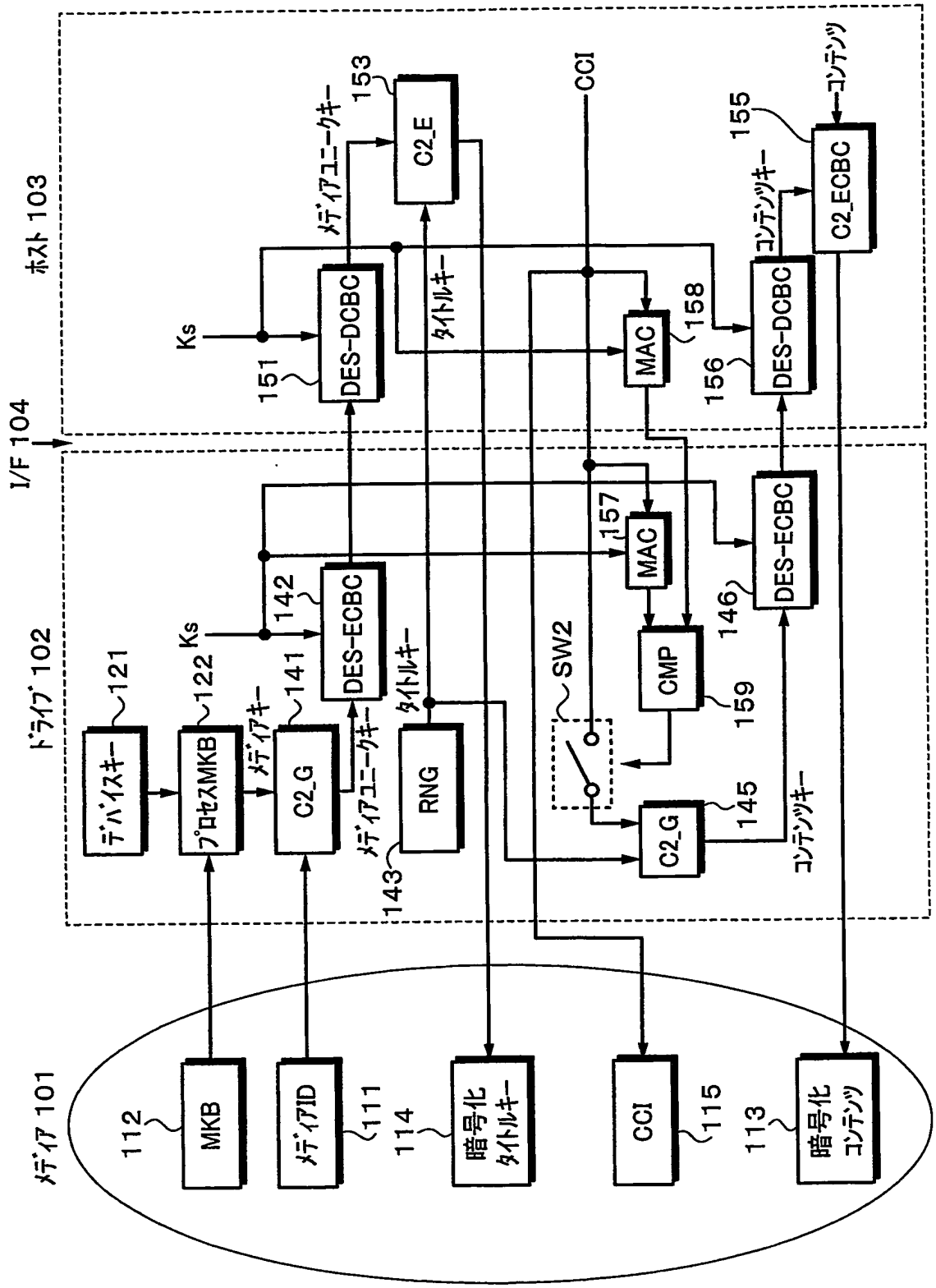
第１０図


メディア 101
ドライブ 102
I/F 104
ホスト 103
112
MKB
111
メディアID
114
暗号化タイトルキー
115
CCI
113
暗号化コンテンツ
121
デバイスキー
122
プロセスMKB
141
C2_G
142
DES-ECBC
Ks
メディアキー
メディアユニークキー
151
DES-DCBC
Ks
メディアユニークキー
153
C2_D
タイトルキー
CCI
154
C2_G
コンテンツキー
155
C2_DCBC
コンテンツ

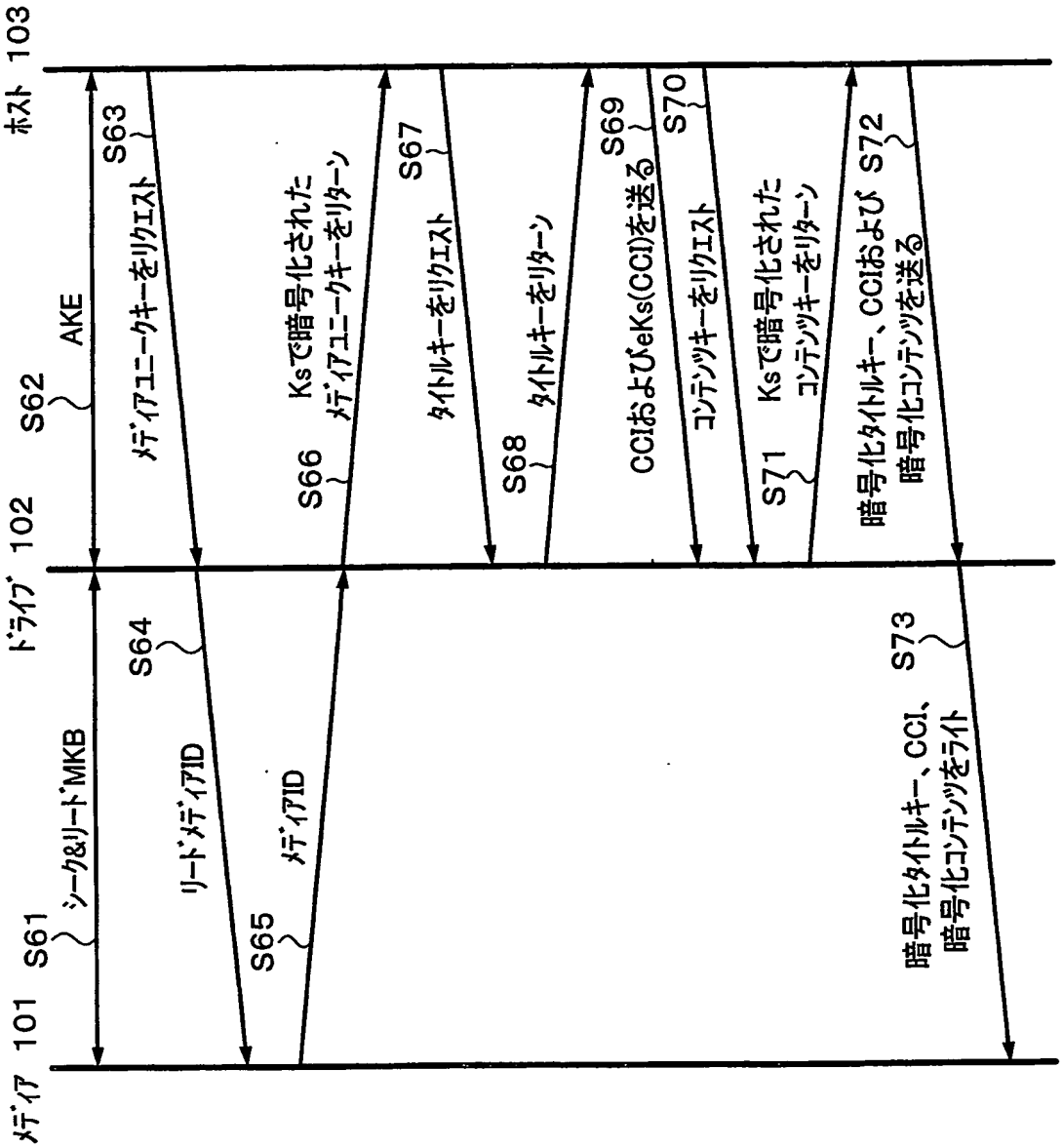
第１１図


ホスト 103
ドライブ 102
メディア 101
S41
シーク&リード'MKB
S42
AKE
S43
メディアユニークキーをリクエスト
S44
リード'メディアID
S45
メディアID
S46
メディアユニークキーをリターン
S47
暗号化タイトルキー、CCI、
暗号化コンテンツをリクエスト
S48
暗号化タイトルキー、CCI、
暗号化コンテンツをリード'
S49
暗号化タイトルキー、CCI、
暗号化コンテンツ
S50
暗号化タイトルキー、CCI、
暗号化コンテンツをリターン

第１２図


メディア 101
MKB
112
メディアID
111
暗号化タイトルキー
114
CCI
115
暗号化コンテンツ
113
I/F 104
ドライブ 102
デバイスキー
121
プロセスMKB
122
メディアキー
C2_G
141
メディアユニークキー
RNG
143
タイトルキー
DES-ECBC
142
Ks
SW2
MAC
157
CMP
159
C2_G
145
DES-ECBC
146
コンテンツキー
ホスト 103
メディアユニークキー
C2_E
153
CCI
Ks
151
DES-DCBC
タイトルキー
MAC
158
156
DES-DCBC
コンテンツキー
C2_ECBC
155
コンテンツ

第１３図


メディア 101
ドライブ 102
ホスト 103
S61
シーク&リード'MKB
S62
AKE
S63
メディアユニークキーをリクエスト
S64
リード'メディアID
S65
メディアID
S66
Ksで暗号化された
メディアユニークキーをリターン
S67
タイトルキーをリクエスト
S68
タイトルキーをリターン
S69
CCIおよびeKs(CCI)を送る
S70
コンテンツキーをリクエスト
S71
Ksで暗号化された
コンテンツキーをリターン
S72
暗号化タイトルキー、CCIおよび
暗号化コンテンツを送る
S73
暗号化タイトルキー、CCI、
暗号化コンテンツをライト

符号の説明

1	ＤＶＤメディア
2	レコーダ
3	プレーヤ
4	ＤＶＤドライブ
4ａ	インターフェース
5	ホスト
１１	メディアＩＤ
１２	メディアキーブロック（ＭＫＢ）
１３	暗号化コンテンツ
４２，５２	ＭＡＣ演算ブロック
４６	デバイスキー
４６ａ	デバイスキーの前半部.
４７	ＤＥＳエンクリプタ
４８	メディアユニークキー演算ブロック
４９，４９ａ	ＤＥＳエンクリプタ
４９ｂ	ＤＥＳデクリプタ
５３	ＭＡＣを比較する比較
５４	暗号化／複合モジュール
５５	メディアユニークキー演算ブロック
１０１	メディア
１０２	ドライブ
１０３	ホスト
１０４	インターフェース
１２１	ドライブのデバイスキー

122　プロセスＭＫＢ

123、124、125　ドライブのＭＡＣ演算ブロック

126、127、128　ドライブの乱数発生器

129　比較

131　ホストのデバイスキー

132　プロセスＭＫＢ

133、134、135　ホストのＭＡＣ演算ブロック

136、137、138　ホストの乱数発生器

139　比較

141、154　Ｃ２＿Ｇ

142、144　ＤＥＳエンクリプタ

143　乱数発生器

151、152、156　ＤＥＳデクリプタ

153　Ｃ２＿Ｅ

155　Ｃ２＿ＥＢＣ

157、158　ＭＡＣ演算ブロック

159　比較

ＳＴ１　ＭＡＣ計算値が一致？

ＳＴ２　スイッチをＯＮ

ＳＴ３　スイッチをＯＦＦ

ＳＴ１０　ＲＥＰＯＲＴ　ＫＥＹ（ＭＫＢ）

ＳＴ１１　メディアキーＫｍを計算

ＳＴ１２　リボーク？

ＳＴ１３　ＲＥＣＥＩＶＥ（Ｒｂ１，Ｒｂ２）

ＳＴ１４　ＲＥＴＵＲＮ（eＫｍ(Ｒａ１‖Ｒｂ１)，Ｒａ１）

ＳＴ１５　ＲＥＴＵＲＮ（Ｒａ２，Ｒａ３）

ＳＴ１６　ＲＥＣＥＩＶＥ
(eKm(Rb2 ‖ Ra2), Rb3)

ＳＴ１７　同一のＭＡＣ？

ＳＴ１８　セッションキーの確定
(eKm(Ra3 ‖ Rb3))

ＳＴ１９　ＲＥＴＵＲＮ（エラー）

ＳＴ２０　ＲＥＰＯＲＴ　ＫＥＹ（ＭＫＢ）

ＳＴ２１　メディアキーＫｍを計算

ＳＴ２２　リボーク？

ＳＴ２３　ＳＥＮＤ　ＫＥＹ（Rb1, Rb2）

ＳＴ２４　ＲＥＰＯＲＴ　ＫＥＹ
(eKm(Ra1 ‖ Rb1), Ra1)

ＳＴ２５　同一のＭＡＣ？

ＳＴ２６　ＲＥＰＯＲＴ　ＫＥＹ.(Ra2, Ra3)

ＳＴ２７　ＳＥＮＤ　ＫＥＹ
(eKm(Rb2 ‖ Ra2), Rb3)

ＳＴ２８　エラー？

ＳＴ２９　セッションキーの確定
(eKm(Ra3 ‖ Rb3))

INTERNATIONAL SEARCH REPORT

International application No.
[redacted]/JP03/16226

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/32, G11B20/10, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/32, G11B20/10, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS), content, mutual, authentication, MKB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-331106 A (Matsushita Electric Industrial Co., Ltd.), 30 November, 2001 (30.11.01), Par. Nos. [0099] to [0115] & EP 1134964 A1 & CN 1313599 A & KR 2001092320 A & US 2002/0015494 A1 & TW 529020 A	1-9,24,25
Y	Makoto TATEBAYASHI et al., "Kiroku Media no Contents Hogo System", 2000 Nen The Institute of Electronics, Information and Communication Engineers Kiso Kyokai Society Taikai Koen Ronbunshu, 07 September, 2000 (07.09.00), pages 367 to 368, 2.2 MEB o Mochiita Kagi Mukoka System, 4.2 Dosa Gaiyo	1-9,24,25

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
26 April, 2004 (26.04.04)

Date of mailing of the international search report
18 May, 2004 (18.05.04)

Name and mailing address of the ISA/
Japanese Patent Office

Facsimile No.

Authorized officer

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
[redacted]T/JP03/16226

Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☒ Claims Nos.: 10-23
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号　PCT／JP03／16226

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L9／32, G11B20／10, G06F12／14

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L9／32, G11B20／10, G06F12／14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JICSTファイル（JOIS）
content, mutual, authentication, MKB

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2001-331106 A (松下電器産業株式会社) 2001.11.30, 第99-115段落 & EP 1134964 A1 & CN 1313599 A & KR 2001092320 A & US 2002/0015494 A1 & TW 529020 A	1-9, 24, 25
Y	館林誠 他, 記録メディアのコンテンツ保護システム, 2000年電子情報通信学会基礎・境界ソサイエティ大会講演論文集, 2000.09.07, p.367-368, 2.2 MKBを用いた鍵無効化システム, 4.2動作概要	1-9, 24, 25

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　26.04.2004	国際調査報告の発送日　18.5.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　5M　9364 中里　裕正 電話番号　03－3581－1101　内線　3597

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号ＰＣＴ／ＪＰ０３／１６２２６

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☒ 請求の範囲 10-23 は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。